NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A PROPOSED COSMOLOGY OF IDENTITY IN THE SOCIOTECHNICAL ECOSYSTEM OF HOMELAND SECURITY

by

Sevan D. Gerard

December 2017

Thesis Advisor:	Rodrigo Nieto-Gomez
Second Reader:	Christopher Bellavita

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE A PROPOSED COSMOLOGY OF IDENTITY IN THE SOCIOTECHNICAL ECOSYSTEM OF HOMELAND SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Sevan D. Gerard	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis explores how identity and technology interact in the context of terrorism and conflict. This relationship is important to understand because technology can be designed to shape identity and drive behavior. This ability to manipulate identity through technological means has ethical implications for technological innovation and design and can lead to emerging threats in homeland security. This thesis uses the position of soldier as a template to develop an understanding of the most basic social functions, which are technologically dependent. Following the analysis, the thesis builds a framework called the sociotechnical ecosystem based on artifact, mobility, communications, information, and network structures. Finally, this thesis proposes a new conceptual model to provide a mechanism for analyzing the influence a technological environment can exert on social identity.

14. SUBJECT TERMS identity, social identity theory (SIT), sociotechnical ecosystem, sociotechnical identity, homeland security, terrorism, conflict, sociology, technology, information, artifact, mobility, communication, network structure, technoself, technium	**15. NUMBER OF PAGES** 105
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A PROPOSED COSMOLOGY OF IDENTITY IN THE SOCIOTECHNICAL ECOSYSTEM OF HOMELAND SECURITY

Sevan D. Gerard
Firefighter/Paramedic, Los Angeles Fire Department
B.S., Loma Linda University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2017**

Approved by: Rodrigo Nieto-Gomez
Thesis Advisor

Christopher Bellavita
Second Reader

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores how identity and technology interact in the context of terrorism and conflict. This relationship is important to understand because technology can be designed to shape identity and drive behavior. This ability to manipulate identity through technological means has ethical implications for technological innovation and design and can lead to emerging threats in homeland security. This thesis uses the position of soldier as a template to develop an understanding of the most basic social functions, which are technologically dependent. Following the analysis, the thesis builds a framework called the sociotechnical ecosystem based on artifact, mobility, communications, information, and network structures. Finally, this thesis proposes a new conceptual model to provide a mechanism for analyzing the influence a technological environment can exert on social identity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

Anon	Anonymous
ANT	actor-network theory
FBI	Federal Bureau of Investigation
IED	improvised explosive device
IoT	Internet-of-Things
ISIS	Islamic State of Iraq and Syria
MMOG	massively multiplayer online game
SCOT	social construction of technology
SIT	social identity theory
STIT	sociotechnical identity theory

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The thesis explores how technology and social identity interact in the context of homeland security. Emerging ideas on technologically dependent and enhanced humans raise important ontological questions about current theories of identity, culture, and society and how a new identity paradigm creates security threats.[1] There is currently no agreement on the fundamental nature or properties of the relationship between humans and technology, an interface ontology of sorts, but entire fields, like technoself studies, are emerging to try to understand this relationship.[2]

The threats to homeland security are still evolving, and key sociotechnical issues, such as genetic manipulations, issues of privacy and surveillance, human enhancements, virtual identity, online anonymity, social-media mobilization, and the global decentralization of terrorist groups, all create new threats requiring innovative informed analysis to manage. The topics of identity and human behavior are certainly not unfamiliar to homeland security, but the analytical methodologies to study identity have focused primarily on psychological and sociological definitions or economic and political factors. In the face of this evolving interdependence and deepening hybridization of human and machine, what we know and how we study identity is being significantly altered.

This thesis explores ideas surrounding the interface of social groups and technology in an attempt to develop better analytical tools for the study of social identity within homeland security. It evaluates traditional academic perspectives, which are combined and contrasted to distill important themes to contemporary thought on human-machine amalgamation.

---

[1] Rodrigo Nieto Gómez, "This Is Your Brain on Code: Embodied Intelligence Augmentation and Conflict," in *Augmented Intelligence: Smart Systems and the Future of Work and Learning*, ed. Daniel Araya (New York: Peter Lang, 2018), forthcoming.

[2] Rocci Luppicini, "The Emerging Field of Technoself Studies (TSS)," in *Handbook of Research on Technoself: Identity in a Technological Society*, ed. Rocci Luppicini, 1–25 (Hershey, PA: IGI Global, 2012), 2–3.

An extensive literature review identifies a large gap in the fundamental organization of thoughts surrounding technological identity. As a result, this research includes an inductive inquiry in an attempt to build a fundamental ontological blueprint for the concept of a sociotechnical ecosystem. The intent of developing a framework for a sociotechnical ecosystem is to provide a technology dependent sociological system of reference, which can be used to understand or estimate the nature of a specific social group's technological identity or dependence, and how its behavior is shaped by the technological context.

To assist in the development of this framework, this thesis uses the concept of the soldier to begin extrapolating what will become the dimensions of the soldier's sociotechnical ecosystem. The "Army Warrior Tasks," as defined by the U.S. Army Training and Doctrine Command, states that soldiers, who are considered here as sociotechnical beings, need to "shoot, move, communicate, survive, and adapt."[3]

From this military example, one can deduce that several core dimensions are driving the soldiers' operational environment, which will come to define their sociotechnical ecosystem. Soldiers require weapons—in other words artifacts, mobility, the ability to communicate, information about tactics, strategy and core knowledge, and finally, they need to be organized into a larger system of social structures, a network structure that categorizes them both as subordinates within their organization and enemies to a foe. Combined, these dimensions of artifact, mobility, communication, information, and network structure form the scaffolding of sociotechnical ecosystems. As with any ecosystem, sociotechnical ones also need to constantly evolve and adapt to survive. The principles distilled from the position of soldiers are not exclusive to a military or homeland security context. The consideration of a multitude of positions or social groups yields the existence of the identical dimensions for other ecosystems.

Applying this concept to the study of homeland security requires the combination of an effective framework for studying identity with this new proposed ecosystem. Social

[3] U.S. Department of the Army, *Basic Officer Leader Training Policies and Administration* (TRADOC Regulation 350-36) (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2015), http://www.tradoc.army.mil/tpubs/regs/TR350-36.pdf.

identity theory offers a strong analytical approach for studying social conflict and terrorism and is therefore the preferred framework to build upon. The combined use of these two frameworks give the study of identity a deeper reach into the mutual influences of ingroup narrative and technological identity, and as a combined framework has been given the name "sociotechnical identity theory."

The fundamental intention of this thesis is not to think of technology in terms of the potential threats it may present to critical infrastructure, privacy, or user safety, but rather the important influence it has on identity itself. Rather than focusing on the unintended consequences of technology from a utilitarian perspective, homeland security practitioners need to consider the intended consequences of technology adoption on human identity and behavior. Deep consideration must be given to the ways a technological environment can be leveraged to undermine national and group identity, how it influences the sense of self, and the impact it has on psychological well-being. Finally, it is also critical to maintain a sharp focus on understanding all the ethical implications of sociotechnical innovation and design when used to alter human identity.

To support effective analysis of the threats of intentional identity manipulation through technological means, this thesis concludes by recommending the use of sociotechnical identity theory, the amalgamation of social identity theory and the sociotechnical ecosystem, as an analytical methodology when studying social categorization and behavior in the context of conflict, terrorism, and homeland security at large to capture the influence that technology, in all its forms, has on social identity.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I cannot begin to express enough the deep gratitude I feel for the support, mentoring, and cognitive enrichment that the Center for Homeland Defense and Security at the Naval Postgraduate School has brought me. This started with all the members of cohorts 1503 and 1504, all of whom I now consider my extended family and feel excited about sharing grand ideas with going forward. I want to thank each and every member of the faculty as well as the incredible guest speakers who took the time to come out and share their wealth of knowledge and experience with us. I need to thank Dave Brannan and Anders Strindberg for introducing me to social identity theory and Richard Bergin for discussing sociotechnical systems during the course of our studies. I think these ideas collided in my head with such resonance that it led to the subject of this thesis.

Next, I would like to give special attention to acknowledge the support, mentorship, and incredible patience of my thesis advisor and second reader. Chris Bellavita, thank you for providing me with an incredible telephone conversation right at the beginning of the program, which was so unconventional, complex, and tangentially brilliant, that I immediately knew I had come to the right place. Thank you for your wise words in helping me feel that philosophy does have a place in homeland security, albeit somewhere far out and secluded.

Rodrigo Nieto-Gomez, I have so many words I want to use to attempt to describe the impact you have had both on my thesis and my academic growth; you worked so hard throughout the thesis to make me cut the mountains of text down to precise, succinct, and essential words, so I will at least honor it here. I couldn't have done this without your advice and guidance, so my thanks can only follow exponential growth. You are a friend, an inspiration for self-improvement, and a true mentor.

Lastly, I want to thank my family for their support. I thank my parents for always teaching me the value of education even though it was a really rough road for them until I reached college. I am infinitely grateful to my partner in life, Zoe, for always believing in me and my ability to pull off the conceptual contortion required for this thesis to come

together. Thank you for your sacrifice and patience in waiting for me to finally finish this work.

And to my daughter, Kalea, your very nature, curiosity, and spirit has made me want to become a better human. That manifested into the perseverance necessary to pull through and complete this thesis. Thank you.

I. THE BLUEPRINT

This thesis answers the following question: how do technology and social identity interact in the context of homeland security?

A. PROBLEM STATEMENT

Technology and humankind have evolved over time into an intertwined codependence, each facilitating and enhancing the other's capacity to engage and influence its environment. Over the last few centuries, many disciplines have explored the interaction between humans and technology, with interests ranging from the Paleolithic archeological studies of the Stone Age to contemporary futurists theorizing on a hybridization of humans and machines.[1] Emerging ideas on technologically dependent and enhanced humans raise important ontological questions about current theories of identity, culture, and society and how a new identity paradigm creates security threats.[2] There are currently no accepted conclusions resulting from the exploration of an interface ontology between human and machine, but the field of technoself studies is entering the global parlance as an "interdisciplinary field of research concerned with all aspects of human identity and alteration within a technological society."[3] The term technoself has come to denote a variety of views on "what constitutes humans as beings with a technological nature [that] include, but are not limited to the following: cyborg, beman (bio-electric human), posthuman, transhuman, technohuman, digital identity, avatars, and homotechnicus."[4]

---

[1] *Encyclopedia Britannica*, s.v. "Anthropology/Stone Age," accessed October 15, 2016, https://www.britannica.com/event/Stone-Age; Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Penguin Books, 2005), 317.

[2] Rodrigo Nieto Gómez, "This Is Your Brain on Code: Embodied Intelligence Augmentation and Conflict," in *Augmented Intelligence: Smart Systems and the Future of Work and Learning*, ed. Daniel Araya (New York: Peter Lang, 2018), forthcoming.

[3] Rocci Luppicini, "The Emerging Field of Technoself Studies (TSS)," in *Handbook of Research on Technoself: Identity in a Technological Society*, ed. Rocci Luppicini, 1–25 (Hershey, PA: IGI Global, 2012), 2–3.

[4] Rocci Luppicini, *Handbook of Research on Technoself: Identity in a Technological Society* (Hershey, PA: IGI Global, 2012), 4.

While marketing research has traditionally focused on the interaction between humans and machines, the current environment leads us to ask whether technology has actually become an integrated facet of identity with the degree of influence on behavior traditionally attributed to psychology and sociology. As the field of technoself studies is just developing, there is currently no mention or reference to it within the homeland security literature. The threats to homeland security are still evolving and key sociotechnical issues, such as genetic manipulation, issues of privacy and surveillance, human enhancements, virtual identity, online anonymity, social media mobilization, and the decentralization of terrorist groups create new threats and demand informed analysis. However, homeland security as a discipline tackles technology through a utilitarian lens, focusing, for example, on specific threats from cybersecurity, autonomous vehicles, and weapons of mass destruction while giving little consideration to how technologies are modifying human behavior and identity.[5]

The topics of identity and human behavior are certainly not unfamiliar to homeland security, but the analytical methodologies to study identity within the context of homeland security have focused primarily on psychological and sociological definitions, including economic and political factors. For example, Jessica Stern, a research professor at Boston University and member of the Aspen Homeland Security Advisory Group, wrote a paper exploring individual mobilization to extremist violence based on "what we know about the psychological and social factors motivating young people to join extremist groups."[6] The consistent use of these two disciplines is made even more evident by the results of an online search for the terms "understanding terrorism" and "factors that cause terrorism," which both make persistent reference to psychological and sociological factors.[7] While group identity is the product of

[5] Weapons of mass destruction (WMDs) are categorized into chemical, biological, radiological, nuclear and explosive weapons (CBRNE). These two abbreviations are often used interchangeably.

[6] Jessica Stern, "Radicalization to Extremism and Mobilization to Violence: What Have We Learned and What Can We Do about It?," *The Annals of the American Academy of Political and Social Science* 668, no. 1 (2016): 102–117.

[7] The search engine Google was used for both terms and yielded numerous references to "psychological," "social," "economic," and "political" without notable reference to the term "technological."

interactions between individuals and the socially constructed narratives they exchange, the technological environment in which these groups exist also has a tremendous influence on shaping group narratives and therefore group identity.[8] Unfortunately, this technological impact on identity remains understudied.

This thesis explores theories on identity through emerging studies on human-technological interaction in an attempt to better understand the concept of a sociotechnical identity. This thesis adapts the analytical frame of social identity theory (SIT) into a framework encompassing both social identity and technological identity within the context of homeland security. This was done by broadly defining a new system titled the sociotechnical ecosystem so as to facilitate sensemaking of self-categorization in complex technologically dependent environments. This approach no longer considers technology as a set of simple enabling tools but rather an active participant in driving identity and the resulting human threats to homeland security.

The thesis first considers how technology exists beyond its simple physical representations as a dimension or extension of human identity and what influence that exerts on human behavior. This requires an exploration of what is known about the nature of technology, about sociotechnical systems, and what essential purposes technology fulfills for society. Understanding these aspects as technological dimensions helps to frame functional boundaries for a sociotechnical ecosystem. This thesis uses the military as an example of a sociotechnical ecosystem blueprint to define a framework of sociotechnical ecosystems.

B. LITERATURE REVIEW

The purpose of this literature review is to identify and explore sources of thought applying to key areas of the thesis: technological ecosystems, technoself studies, and the current tools we have to study social identity. This review attempts to focus on areas applicable to homeland security since the intended goal of this thesis is to develop an

[8] Peter Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (London UK: Penguin Books Ltd, 1966). The authors purport that reality is socially constructed and that therefore it is subjectively defined and accepted by a group. The subjective experience of reality, which leads to the definition of self, is rooted in and dependent upon the subject's environment.

improved analytical framework for understanding identity in complex sociotechnical environments.

1. Identity and the Technoself

Technoself studies was first introduced by Lupiccini in 2013 in reference to an emerging multidisciplinary academic domain focused on questions of human identity in sociotechnical environments.[9] Since technology is highly dynamic and exponentially evolving, a new framework of study is necessary to map and analyze the assimilation and incorporation of technologies within humans. Technoself studies focus on the transformation of identity rather than pursuing a preoccupation with specific technical innovations. Luppicini employs the term *technoself* in reference to the transformation of human identity as a result of the adoption or permeation of emerging technologies into the physiological, psychological, and social fabric of humankind.[10] This permeation may occur through the implantation of prosthetics, through biomedical and genetic modifications, or through the external use of new technologies modifying behavior and influencing biological adaptation to new processes and experiences. Susan Greenfield, research groups from Massachusetts Institute of Technology, Harvard, and many others have begun conducting research on the effects of technological use on the physical brain.[11] The research and understanding of brain plasticity keeps improving, and it is revealing that technology is physically remodeling the electrical pathways inside our brains.[12] These modifications to the anatomical structures of the central nervous system are the result of behavior modification and are therefore indirect consequences on individual technological adoption. The same literature points to unintended consequences

[9] Luppicini, "The Emerging Field of Technoself," 1.

[10] Ibid., 4.

[11] Susan Greenfield, *Mind Change: How Digital Technologies Are Leaving Their Mark on Our Brains* (New York: Random House Publishing Group, 2015).

[12] Carolyn Gregoire, "The Internet May Be Changing Your Brain in Ways You've Never Imagined," *The Huffington Post*, October 9, 2015, http://www.huffingtonpost.com/entry/internet-changing-brain-nicholas-carr_us_5614037de4b0368a1a613e96; Rebecca Hiscott, "8 Ways Tech Has Completely Rewired Our Brains," *Mashable*, March 14, 2014, http://mashable.com/2014/03/14/tech-brains-neuroplasticity/; "How the Internet Is Changing Your Brain," Academic Earth, accessed July 8, 2016, http://academicearth.org/electives/internet-changing-your-brain/.

resulting from technological utilization, including reduced memory, increased distraction, and addictive behavior.

In addition to direct physiological enhancements through the bio-integration of technology and the indirect structural changes to technology adopters resulting from their technology dependent behaviors, the topic of digital identity also raises essential questions on matters of personal identity. The concepts are quite broad, encompassing questions of virtual anonymity, the creation and relation to personal avatars, self-presentation, disinhibition, and Doppelganger bots, for example, but they have been included in the discussion to help in understanding the spectrum of the concept of a *technoself*.[13]

2. On the Intersection of Sociology and Technology

The first step in exploring the subject of this thesis is to define the terms selected. The word *ecosystem* was specifically selected for this context to capture what the *Oxford Dictionary* defines as "a biological community of interacting organisms and their physical environment, or a complex network or interconnected system."[14] This definition suggests that society and technology share an inextricably connected environment. In the context of this thesis, the term technology must be understood beyond its simple physical manifestation as objects and tools. A better term in this context to describe the intended technological nature of a specific social environment is the term *technicity*. The intended definition here is best described by *Wiktionary*, which defines *technicity* as "the efficacy, functionality, or experience of a particular technology; the prevalence of or reliance upon (a particular) technology by a specific group of people or by humanity as a whole."[15] From here on, the term technicity refers to the technical dimensions, whether physical, conceptual, organizational, or other of any chosen environment.

---

[13] Oana Goga, Giridhari Venkatadri, and Krishna P. Gummadi, "The Doppelgänger Bot Attack: Exploring Identity Impersonation in Online Social Networks," in *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, 141–153 (New York: ACM, 2015).

[14] *Oxford Dictionaries*, s.v. "Ecosystem," accessed October 15, 2016, https://en.oxforddictionaries.com/definition/us/ecosystem.

[15] *Wiktionary—The Free Dictionary*, s.v. "Technicity," accessed October 15, 2016, https://en.wiktionary.org/wiki/technicity.

The term *sociotechnical systems* was first coined in the 1940s by Eric Trist, Ken Bamforth, and Fred Emery based on their work at the Tavistock Institute in London with English coal miners.[16] Today, the term is used in business in reference to the "interaction between society's complex infrastructures and human behavior."[17] Following the introduction of the term and field of study, several other subdisciplines emerged focusing predominantly on organizational dynamics, management sciences, and social engineering.[18] Vojinović and Abbott define *sociotechnology* as "the study of processes in which the social and the technical are indivisibly combined."[19] Wiebe Bijker, a Dutch professor of technology and society, wrote of sociotechnical change that "Society is not determined by technology, nor is technology determined by society. Both emerge as two sides of the sociotechnical coin."[20] This implies a heterogenic interaction between the two systems, which does not account for the evolutionary interdependence between society and technology more frequently voiced today. In his 1976 work *The Hunting Hypothesis,* paleoanthropologist Robert Ardrey points out that the development of stone tools approximately 2.5 million years ago led society into the Stone Age, which in turn was instrumental in turning humans into hunters.[21] This is one example of many cyclical evolutionary spurts led by the synergistic relationship between society and technology. This is the specific interest of the *technology and society* school, which is founded on the cyclical codependence between culture and technology.

---

[16] Frederick Edmund Emery, *Characteristics of Socio-Technical Systems: A Critical Review of Theories and Facts* (London: Tavistock Institute of Human Relations, 1959), Document 527.

[17] *Wikipedia*, s.v., "Sociotechnical System," July 2, 2017, https://en.wikipedia.org/w/index.php?title=Sociotechnical_system&oldid=788670547.

[18] David John Farmer, *The Language of Public Administration: Bureaucracy, Modernity, and Postmodernity* (Tuscaloosa, AL: University of Alabama Press, 1995), 95.

[19] Zoran Vojinović and Michael B. Abbott, *Flood Risk and Social Justice: From Quantitative to Qualitative Flood Risk Assessment and Mitigation* (London: International Water Association Publishing, 2012), 164.

[20] Wiebe E. Bijker, Thomas P. Hughes, and Trevor J. Pinch, eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987), 274.

[21] Robert Ardrey, *The Hunting Hypothesis: A Personal Conclusion Concerning the Evolutionary Nature of Man* (London: Macmillan Pub. Co, 1976), 231.

Historically, research on the ontology of technology has been highly reductionist and divided scholars into either social constructivists or technological determinists. Technological constructivism, also referred to as the social construction of technology (SCOT), is the theory that human actions drive the development of technology.[22] This suggests an understanding of how technology is used and applied is dependent on an understanding of its social context. On the other end is technological determinism, a term first attributed to Thorstein Veblen around the 1900s, and it presumes that a "society's technology drives the development of its social structure and cultural values."[23] Technological determinism was later molded into the theory of mass media by McLuhan in 1964.[24] McLuhan proposed that the evolution of media technologies from tribal communication, to literacy, to print, to digital communications has changed how society experienced reality and therefore how technology drove the evolution of social culture.[25]

More recently, the exponential developments in computing and the decreasing physical scales in hardware have led to an organic approach to studying technological systems. Authors like Brian Arthur and Kevin Kelly approach technology as living and evolving organisms, or in Kevin Kelly's terms a "living kingdom."[26] In *The Nature of Technology*, Brian Arthur conducts an analysis using a systems approach to deconstruct and understand the physical manifestation of phenomena.[27] He suggests that technology is combinatorial and is subject to its own evolution. By encompassing all physical manifestations of phenomena as evolving technology, Arthur supports the hypothesis of Kevin Kelly's *Technium*, which Kelly defines as "the greater, global, massively interconnected system of technology vibrating around us."[28] In addition, Kelly defines

---

[22] *Wikipedia*, s.v., "Social Construction of Technology," August 23, 2016, https://en.wikipedia.org/w/index.php?title=Social_construction_of_technology&oldid=735873197.

[23] *Wikipedia*, s.v., "Technological Determinism," September 14, 2016, https://en.wikipedia.org/w/index.php?title=Technological_determinism&oldid=739447974.

[24] Marshall McLuhan, *Understanding Media* (New York: McGraw-Hill, 1964).

[25] Ibid.

[26] Kevin Kelly, "The Technium and the 7th Kingdom of Life," Edge, July 18, 2007, https://www.edge.org/conversation/kevin_kelly-the-technium-and-the-7th-kingdom-of-life.

[27] Brian W. Arthur, *The Nature of Technology: What It Is and How It Evolves* (New York: Simon and Schuster, 2009).

[28] Kevin Kelly, *What Technology Wants* (New York: Penguin Group, 2010), 11.

technology as a living force, which, using biological taxonomy, he categorizes as the seventh living kingdom. He further posits that technology evolves under a set of multiple environmental forces and constraints, which like most living systems is emergent and adapts exponentially. In another publication called *Out Of Control*, Kelly touches on the biology of machines making a correlation between traditional biological models and technology.[29] In Kelly's words

> Technology is the phenotype of mind. It is the body for ideas. And what is remarkable about this body is that taken as a whole, it resembles the phenotype of biology. While there are some differences, the evolution of technology mimics the evolution of life. The two share many traits: both evolutions move from simple to complex, from generalism to specialism, from uniformity to diversity, from individualism to socialism, from energy waste to efficiency, and from slow change to greater evolvability. Technology, like biology, moves toward greater diversity, socialism, complexity, efficiency and evolvability.[30]

As a living kingdom, technology would be subject to interspecies symbiosis, parasitism, competition, or recombination. Advances in biotechnology and the human incorporation of technology for survival and enhancement support this view and give rise to the concept of a technoself, which is described in the next section.

In this advanced technological period of discovery and innovation, we are seeing significant changes in the degree of usage and integration of technology in the social paradigm. Whether it is the use of social network platforms, prosthetics, biometrics, or the Internet-of-Things (IoT), our technological ecosystem transforms our natural environment and as a result technology and people are hybridizing.[31] As a strong proponent of the artificial intelligence *singularity* and the transhumanism of human-machine merger, Kurzweil suggests that technology and humans will ultimately end as competitors, while Kelly holds stronger to the cooperative amalgamation of the two—a

---

[29] Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*, reprint (New York: Basic Books, 1995).

[30] Kevin Kelly, "The Technium: The Seventh Kingdom," KK, February 1, 2006, http://kk.org/thetechnium/the-seventh-kin/.

[31] "What Will the Future Hold for Cyborgs, the Fusion of Humans and Machines?" *ScienceDaily*, July 11, 2013, https://www.sciencedaily.com/releases/2013/07/130711084114.htm.

cyborg future wherein technology and humans fuse into some new entity.[32] In either case, a strong argument can be made regarding the interdependence of technology and human identity.

The concern of homeland security practitioners should be the ubiquity of technological adoption in every aspect of life, which is both facilitating and dictating changes in human behavior. This means that the traditional psychological and sociological perspectives on human behavior and motivation may offer incomplete perspectives on identity. As a strong force acting on identity and human behavior, technology should be more deeply considered, particularly as a paradigm wherein the lines between reality and virtuality are becoming more indistinguishable. Homeland security is particularly affected by technological innovations such as virtual reality, industrial control systems, the IoT, nanotechnology, synthetic biology, genetic engineering, and 3D printing. A new technological type of Kantian lens is necessary to remain mindful of the influence of technology on identity and how that in turn evolves threats to homeland security.

3. Analytical Frames for the Study of Identity in Homeland Security

A 2004 unclassified report by the Norwegian Defense Research Establishment presents a comprehensive review of the causes of terrorism by focusing on the predominant theories explaining motivations and variations in vulnerability to terrorism. The basic framework of the analysis is built on psychological, sociological, and cultural frames available to study terrorist archetypes through contemporary models of individual and group identity.[33] The findings of the report are compatible with the framework of SIT and Henri Tajfel's definition of social identity, which is derived from the combination of an individual's cognition, internal evaluation and emotions.[34] The Defense report lists

[32] Kelly, *Out of Control*; Ray Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence* (New York: Penguin Book, 2000).

[33] Lia Brynjar and SkjØlberg Katja, *Causes of Terrorism: An Expanded and Updated Review of the Literature* (Kjeller, Norway: Norwegian Defense Research Establishment, 2004), https://www.ffi.no/no/Rapporter/04-04307.pdf.

[34] Henri Tajfel, ed., *Differentiation between Social Groups: Studies in the Social Psychology of Intergroup Relations* (London: Academic Press, 1978), 28.

social identity theory as one available framework and supports the selection of that framework in the context of this thesis. The social identity theory framework is especially interesting to the study of terrorism and homeland security because it offers a model to analyze intergroup relations and conflict.[35] Given the preoccupation of the thesis with the technological influence on identity and the resulting human threats to homeland security, this thesis uses SIT as the foundation upon which to build the proposed model.

To test the efficacy and utility of the proposed framework, this thesis considers the terrorist group known as the Islamic State to evaluate whether its sociotechnical ecosystem is a logical marker of the organization's ingroup narrative and behaviors.

C. RESEARCH DESIGN

Multidisciplinary theories are emerging regarding the biological, psychological and sociological impacts of technology on identity, but they have not yet claimed foothold in the homeland security discourse. This research is centered on a new theoretical framework for thinking about the impact of technology on identity and how it may complement social identity theory in the context of homeland security. I call the proposed model sociotechnical identity theory (STIT), and it is composed of two analytical frames: social identity theory and the *sociotechnical ecosystem* model proposed later. These two frames, meant to be considered together, offer a consistent methodology for thinking about the mutual influences of identity and socio-environmental technicity.

I assembled the proposed framework in this thesis following inductive inquiry into academic research in the fields of biology, technology, and sociology, as well as social media analysis. Social identity theory naturally emerged as the preferred analytical framework to start from for the purposes of group analysis because it offers a broad and open-ended methodology, which has already been frequently applied to the analysis of identity relating to conflict and terrorism. The new theory does not purport to offer any definitive or concrete answers but rather reminds anyone conducting analysis to consider social behavior and hermeneutics as fluid, contextually driven, and technologically

[35] David W. Brannan, Kristin M. Darken, and Anders Strindberg, *A Practitioner's Way Forward: Terrorism Analysis* (Salinas, CA: Agile Research and Technology, Incorporated, 2014), 56.

dependent. Therefore, the act of analysis must be ongoing and adaptive to constant change ingroup behavior, norms, values, interests, resources, needs, and most importantly to the question of this thesis, technological environment. Since technology is an inextricable dimension of the social environment, it has to be accounted for in the study of social identity, and this new lens of sociotechnical identity aims to fulfill that demand.

The next chapter dives deeper into the subjects of identity and technology to find a consensus on existing theories and current intersections in subject matter for each. Additionally, this thesis includes a review of contemporary media information to facilitate the understanding of current trends and events in technological innovation as well as terrorism and homeland security. Subsequently, this thesis uses inductive reasoning to attempt to identify gaps and undiscovered symmetries between technological and social behaviors supporting an ontological technicity mediating the experience of humans with nature and toward each other.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PEOPLE AND TECHNOLOGY—A BACKGROUND

> Technology marches in seven-league boots from one ruthless, revolutionary conquest to another, tearing down old factories and industries, flinging up new processes with terrifying rapidity.
>
> Charles Beard[36]

This chapter dives into existing frameworks and theories about technology, its evolution, and its fundamental nature in a sociological context, to synthesize a taxonomy used to define a social group's ecosystem in technological terms. Although there are few certainties with respect to technology, it is conceivable that its nature is inherently dependent on the existence of a user, without which the study of technology could arguably be of no human interest. There are many different ideas on technology spanning the disciplines of philosophy, science, business, and sociology—all attempting to define its nature, which is subsequently summarized and discussed.

In philosophy, technological thinkers are predominantly concerned with questions regarding the nature of technology, how it evolves, where it is headed, and what the implications are to current and future definitions of human existence. Questions of physical identity versus a created virtual online identity, or the ethical implications of human enhancement through biotechnology, are examples of philosophical interest since they bring into question the very nature and boundaries of what we call a human. Scientific inquiry into technology is highly motivated by a desire for problem solving through innovation whereby function and utility tends to precede form. Invention and innovation tend to offer solutions to identified shortcomings while design is tasked with making the product more desirable or universal. In essence, the science of technology is the study of knowledge and organized physical means, whether materialized or shaped as knowledge to alter or "program existing natural phenomena" beyond the natural evolution of energy and matter.[37] Once technology is conceptualized, the business sector

[36] Charles A. Beard, "Time, Technology, and the Creative Spirit in Political Science," *The American Political Science Review* 21, no. 1 (1927): 1–11.

[37] Arthur, *The Nature of Technology*, 203.

rapidly undertakes the design and development of tools to exponentially facilitate the reorganization or control of the so-called phenomena and to influence consumer behavior.

The business sector has developed a significant body of knowledge on sociotechnical systems with a strong focus on process and operation to provide agility in attaining specific desired outcomes.[38] The business imperative is to study how human and machine can combine to make more, better, for less, and faster with the purpose always being maximal productivity measured in revenue. However, this metric of performance falls short when the measurement of success is the human experience.

Finally, the sociological interest in technology focuses on the level of interdependence and mutual influence of technology and society. This section explores the body of ideas on technology as it pertains to the relationship between technology and humans. In the absence of a known framework defining the technological structure of social environments or the domains of a sociotechnical system, I developed a conceptualization of a sociotechnical ecosystem as a starting point to understand the mutual influence and interdependence of archetypical technological categories and social groups. The intent of developing a framework of a sociotechnical ecosystem is to provide a technology dependent sociological system of reference, which can be used to understand or estimate the nature of a specific social group's technological identity or dependence and how its sphere of influence is shaped by the group's technological context. While a sociotechnical system usually follows the reductionist view that a specific set of tasks lead to a desired outcome resulting from human-technological cooperation, the concept of a sociotechnical ecosystem is concerned with identifying and classifying the totality of technological forces encompassing the human experience. The ecosystem perspective focuses on identifying what technicity immerses any given group, which technologies have been adopted or assimilated, which are overtly identified as the

[38] Ken Eason, "Sociotechnical Systems Theory in the 21st Century: Another Half-Filled Glass," in *Sense in Social Science: A Collection of Essays in Honour of Dr. Lisl Klein*, ed. Desmond Graves, 123–134 (Mulgrave, Victoria: Broughton, 2008), http://static1.1.sqspcdn.com/static/f/632322/9574694/1290775147427/Sociotechnical+systems+theory+in+the+21st+Century.pdf?token=Y2DRRODRd4MeBJg9wa%2F2x0L%2B3T8%3D.

social glue or *raison d'être*, and which are categorically rejected. The next sections dive deeper into the nature of technology to help shape the understanding of technology and technicity, which is often stranger than many would think.

A. TECHNOLOGY IS A LIVING SYSTEM

During an interview with American Scientist, Brian Arthur stated,

> I wanted to put an argument out there that technology is alive and let people debate that. Technology passes all the tests for being a living organism—it reproduces itself, it takes in energy and so on. But so far it requires the agency of human beings. One could say, "How could something be living if it requires other organisms for its life?" But human beings are living entities, and we require other organisms ourselves to maintain life.[39]

By his comment, Arthur raises an important point in that there is an inextricable symbiosis between humans and technology. Arthur's argument is well developed in *The Nature of Technology*. He begins with the proposition that "all technologies are combinations of elements; that these elements themselves are technologies; and that all technologies use phenomena to some purpose."[40] This means that technology is subject to a form of combinatorial evolution in which it "creates itself out of itself."[41] In evolving through recombinations of prior technologies, a new one refines and improves itself by occasionally spawning a new "species" of technology by "linking some need to some effect (of effects) that can fulfill it."[42] While humans traditionally have devised the necessary knowledge and information to allow for inventive recombinations, creating new domains of technology, such as computers via processors, technology is now more visibly capable of driving its own combinatorial evolution. People have an intuitive expectation that there is a correlative relationship between technological utilization and its evolution; however, it becomes clear that technology has its own intrinsic developmental properties constrained by the possibility of phenomena and with a degree

[39] Brian Arthur, American Scientist interview, accessed October 15, 2016, https://www.americanscientist.org/bookshelf/pub/an-interview-with-w-brian-arthur.

[40] Arthur, *The Nature of Technology*, 203.

[41] Ibid., 204.

[42] Ibid.

of independence from sociological or human input. If technology has an intrinsic developmental tendency that does not result directly from sociological phenomena, then it can be argued that once developed, adopted, and used, new technologies can influence individual behavior, and therefore society, by imparting characteristics intrinsic to the nature of technology. This premise represents the foundation of the debate between technological constructivism and determinism, which is presented later.

Arthur is not alone in making the argument that technology is akin to a form of life. Kevin Kelly also suggests that technology is a living system, which he calls the technium and proposes as "the seventh kingdom of life" within the taxonomy of life.[43] Kelly defines the technium as "the greater, global, massively interconnected system of technology vibrating around us" and considers the essential quality of the technium to be

> the idea of a self-reinforcing system of creation [where] at some point in its evolution, our system of tools and machines and ideas became so dense in feedback loops and complex interactions that it spawned a bit of independence. It began to exercise some autonomy.[44]

The relevance of Kelly's perspective to this thesis is twofold. First, Kelly suggests that technology, organized into this living force he coins the technium, is instrumental in influencing and expanding human potential. Second, the use of the term technology is too narrow or specific to encompass the dimensional nature he implies in the technium. Technology as a term generally refers to an artifact, a process, some piece of knowledge, or an action, but this fails to encompass the technologically ubiquitous environment within which humanity lives and evolves. Kelly is not the first to identify this dichotomy in the how a technological environment is defined. In 1954, Jacques Ellul wrote *La Technique ou L'Enjeu du Siècle* in which he studied the impact a pan-technological environment exerted on civilization.[45] Ellul's fundamental premise is that the "technique," much like Kelly's technium, is no longer the machine but the environment and atmosphere in which evolved civilizations exist. In Ellul's words

---

[43] Kelly, *Technium Kingdom of Life*.

[44] Kelly, *What Technology Wants*, 11–12.

[45] Jaques Ellul, *La Technique Ou L'enjeu Du Siècle* [The Technological Society], trans. John Wilkinson (New York: Vintage Books. 1967).

> What is called Technique can be assimilated neither to the machine nor to a collection of machines, methods and products. No longer a secondary factor integrated into a nontechnical society and civilisation, Technique has become the dominant factor in the Western world, so that the best name for our society is the "technicist society." It is on technique that all other factors depend. Technique is no longer some uncertain and incomplete intermediary between humanity and the natural milieu. The latter is totally dominated and utilized (in Western society). "Technique now constitutes a fabric of its own, replacing nature. Moreover, technique is the complex and complete milieu in which human beings must live, and in relation to which they must define themselves. It is a universal mediator, producing a generalized mediation, totalizing and aspiring to totality."[46]

Ellul uses the example of a city to illustrate his point. He recognizes that a city is the total displacement of nature, replaced by a complex system of created technologies. In their totality, these form a "milieu," an environment defined by technique. In turn, inhabitants urbanize their lifestyles, sprawl into rural areas or promote "desertification" usually for technical exploitation by a few.[47]

From Ellul's description of *La Technique*, Kelly's description of the *technium*, and Arthur's life-like technological system, it is clear that the developing philosophical frames of technology suggest an inextricable co-evolution between humans and technology and that a metalevel exploration of technology is essential to understand the human experience. Several schools of thought have developed exploring the relationship between technology and humans and generally fall within the domain of science and technology studies.[48]

---

[46] Jacques Ellul, *The Search for Ethics in a Technicist Society*, quoted in Jacques Ellul, "The International Jacques Ellul Society," trans. Dominique Gillot and Carl Mitcham, accessed September 5, 2017, https://ellul.org/themes/ellul-and-technique/. Ellul's emphasis is that technique is really the milieu in which modern humanity is placed.

[47] Ibid.

[48] Socio-technical Systems (CA441 BPM), School of Computing, Dublin City University, November 12, 2013, http://www.computing.dcu.ie/~mcrane/CA441/BP_05_SociotechLectureNotes.pdf; Richard Badham, Chris Clegg, Toby Wall, "Socio-technical Theory," in *International Encyclopedia of Ergonomics and Human Factors*, ed. Waldemar Karwowski (New York: Taylor and Francis, 2001), 1370–1374.

B. SOCIOTECHNICAL SYSTEMS: A LENS SHAPED TO STUDY LABOR?

Sociotechnical systems course notes from the School of Computing at Dublin City University propose that "although the term socio-technical systems is loosely used to describe many complex systems, five key aspect determine a socio-technical system."[49] These are

1. The systems has interdependent parts.
2. The system adapts to and pursues goals in external environments.
3. The system has an internal environment comprising separate but interdependent technical and social subsystems.
4. There is choice in the system (e.g., system goals achievable by more than one means).
5. System performance depends on jointly optimizing the technical and social aspects of the system.[50]

The subject of sociotechnical systems was introduced by the Tavistock Institute as a tool to analyze the mechanization of human labor through industrial, engineering, and manufacturing processes. Today, the system framework if still relevant to many professional disciplines and articulates around the "collaboration of computer hardware, software and people ... designed to meet some business goal."[51] The influence of organizational structures and human participation within technological systems have a strong influence on outcomes. While a purely technological system yields deterministic outcomes, human participation in sociotechnical systems results in emergent properties, which are generally non-deterministic and complex.[52] Sociotechnical systems are foundational to the framing of sociotechnical ecosystems, and the five key aspects listed in these systems also apply within the ecosystem framework.

---

[49] Ibid.

[50] Ibid.

[51] Winifred Glenn, "Chapter 10—Sociotechnical Systems," accessed October 15, 2016, http://slideplayer.com/slide/6671694/.

[52] Ibid.

C. THE THREAT OF TECHNO-REDUCTIONISM: CONSTRUCTIVISM, DETERMINISM, AND ACTOR-NETWORK THEORY

Social constructivism posits that all reality is created, whether metaphysically, epistemologically, or semantically, rather than discovered.[53] Therefore, the constructivist view offers a rebuttal to the idea that society and technology are interdependent in defining the concept of identity. Furthermore, since it supposes that all reality is socially created, then all technology, past, present, and future is created and designed according to the will of social forces. The theory that technology is shaped by social forces is referred to as the SCOT and falls within science and technology studies.[54] SCOT advocates suggest "that technology does not determine human action, but that rather, human action shapes technology. They also argue that the ways a technology is used cannot be understood without understanding how that technology is embedded in its social context."[55]

Conversely, technological determinism, championed by Marx, Kurzweil, Friedman, Ong, and others, suggests that society develops as a function of the technologies it depends on. As defined by *Wikipedia*,

> Technological determinism is a reductionist theory that presumes that a society's technology drives the development of its social structure and cultural values. The term is believed to have been coined by Thorstein Veblen (1857–1929), an American sociologist and economist.[56]

If we look at the historical co-evolution of human societies and technology, we see that neither a constructivist nor deterministic description of the sociotechnical ecosystem answer to all phenomena. The work of paleoanthropologist Robert Ardrey effectively illustrates this through the example of the development of stone tools to facilitate the accomplishment of certain difficult tasks absent the physical attribute of the increased

---

[53] André Kukla, *Social Constructivism and the Philosophy of Science* (London: Routledge, 2000), 4.

[54] Hans K. Klein and Daniel Lee Kleinman, "The Social Construction of Technology: Structural Considerations," *Science, Technology & Human Values* 27, no. 1 (2002): 28–52.

[55] *Wikipedia*, s.v., "Social Construction of Technology."

[56] *Wikipedia*, s.v., "Technological Determinism."

density of stone.[57] This technological development was so useful as a force multiplier that the knowledge rapidly spread and the ubiquitous technological adoption led to the Stone Age. This demonstrates a constructivist technological environment, or in other terms SCOT, wherein the invention by certain members of a social group who distribute the knowledge and capabilities to other members drove the development of the new technological paradigm. The interesting observation that Ardrey makes is that the transition to the Stone Age is what opened the door to a new form of human energy acquisition by allowing a shift from the period of scavenging to such efficient hunting that societies of the Stone Age quickly transitioned into the hunting age.

The ubiquitous adoption of stone tools by the societies of the period led to experimentation and accidental discoveries for new applications of the stone technologies. These previously unthought-of innovations emerged as a result of the physical characteristics of flint, for example. With minimal engineering, it yielded very sharp arrow tips, revealing a new use and power of a natural phenomenon thereby creating new technological knowledge built upon resources originally developed for other purposes. Ardrey's theory suggests that the Stone Age yielded opportunities unique to the essence of the physical properties of the technological paradigm and as a result drove societies to adopt hunting as a means of survival. This teleological explanation of a sociological shift resulting from the characteristics of the technological paradigm falls well within the premise of technological determinism, supporting the idea that technology has the capacity to drive social change. This example is very important because it points to the fact society and technology are entirely codependent and are the result of mutually influential forces.

In keeping with Arthur's idea of technology as a living and evolving system, it becomes evident by the coexistence of constructivist and deterministic tendencies in sociotechnical evolution that there is an inalienable symbiosis between humans and technology. This relationship is certainly not argued, but the constructivist and determinist schools define the symbiosis as parasitic or unilateral.

[57] Ardrey, *The Hunting Hypothesis.*

The constructivists hold that technological development is the product of social forces while the determinists suggest that social change is driven by the technological environment in which people live. However, the relationship is best defined as a mutualistic symbiosis, whereby both domains influence each other's evolution in such a complex way that the forces may at times become indistinguishable from one another. Political scientist Langdon Winner agrees that "in the late twentieth century technology and society, technology and culture, technology and politics are by no means separate."[58] The critical point of these observations is to account for the influence they exert on society and human behavior as technology evolves and begins transcending the limits of the material world into a vast digital and virtual cosmos. Emerging technologies are transcending the ordinary interaction with human senses and users' behavioral outputs, and therefore we need a new mindset to understand how they co-evolve.

Actor-network theory (ANT), which was developed by Callon, Latour, and Law in the 1980s, is an important theory explaining this human-technological interaction.[59] The fundamental principle of ANT is the idea that objects or technologies are integral parts of social networks and that these networks or systems are developed through the participation of both human and nonhuman "actors."[60]

Latour defines an actor as "the name of a movement, a displacement, a transformation, a translation, an enrollment [where] nonhumans lend themselves to social theory as actors, not just vessels of symbolic meaning."[61] Callon and Latour hold that any model of "categorical dualism" is simply theoretical because technology and humanity, just as Descartes's mind and body, are inextricable parts of a whole.

---

[58] *Wikipedia*, s.v., "Science, Technology and Society," September 12, 2016, https://en.wikipedia.org/w/index.php?title=Science,_technology_and_society&oldid=739091860.

[59] *Wikipedia*, s.v., "Actor-network Theory," October 9, 2016, https://en.wikipedia.org/w/index.php?title=Actor%E2%80%93network_theory&oldid=743289904.

[60] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Clarendon Lectures in Management Studies (Oxford: Oxford University Press, 2005), 64.

[61] Ibid.

Law explains the epistemological and ontological position of ANT as consisting of networks, which are defined both by material and semiotic ties.[62] The semiotic and material duality is an important frame to underscore because it implies inclusion of both intrinsic non-material influences of technological elements or technologies as well as the nonlinear influence of human actors with cognitive influence driving social dynamics.

In contrast, Winner criticizes ANT for not attributing agency to either human or nonhuman actors in a network and because it ignores important properties like intent, which is specific to human actors.[63] For this reason, certain scholars criticize ANT for implying networks are "amoral."[64] This question of amorality imposes important legal and homeland security considerations on engineered technologies, such as autonomous vehicles, which could fail or crash as well as be required in the process to select between the safety of the occupants or those outside the vehicle—a case that would let an algorithm determine fatalities.

The challenge following such a predicament is in determining who holds agency in such an outcome. Is it the technologically dependent human in the vehicle, the construction and programing by engineers, or the implementation of policies authorizing the use of such vehicles that would be to blame? Human input leads to unpredictable outcomes in a sociotechnical system, and also it seems likely that the human actor in a network would lead to greater variability in the system than a nonhuman actor in particular social contexts. This question regarding agency demonstrates the tendency of society to want to attribute responsibility to humans for technological failures, thereby not only attributing agency but also morality to humans when it comes to the consequences of technological failures and catastrophes.

---

[62] John Law, "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity," *Systems Practice* 5, no. 4 (1992): 379–393.

[63] Langdon Winner, "Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology," *Science, Technology & Human Values* 18, no. 3 (1993): 362–378.

[64] Ibid.

Stuart Shapiro suggests that using an ecological perspective might provide a methodological way to alleviate the moral dilemma of ANT.[65] The question of agency and morality within the proposed ecosystem is a very important one because with the advent of artificial intelligence and anthropomorphic robots, the technological forces as perceived by humans is becoming more akin to a social interaction than an inorganic use of a tool or facilitating technology. Once again, the biological is becoming more technical, and technology is becoming more human.

So far, this analysis has explored theories and schools of thought touching on the nature of technology and technological environments in the material world to understand the scope of influence the technium has had on people's behaviors. This study provides a backdrop for a framework for an ecosystem perspective of the interaction of humans and their technological environment. It also offers a perspective to reference while exploring the nature and influence of non-material technicity in online, virtual realities. The term "ecology of terrorism" has emerged as an expression focusing on the facilitating circumstances technologies afford certain actors while assuming that motivations or ideologies form independently of technological conditions.[66] This ecological perspective "sees modern terrorism occurring because modern circumstances make terrorist methods exceptionally easy" but does not trigger terrorism in and of itself.[67] However, proponents of this perspective discussed modernization at a time when digital reality was not as ubiquitous. For homeland security, the relative expansion of reality into virtual worlds has deep implications for cybersecurity of course, but it also transforms social interactions and group cohesion, communication among terrorists or criminals, and the capacity to recruit and develop fighters among other things.

Organizations like Islamic State of Iraq and Syria (ISIS) and Anonymous have formed and thrived as technologically improved manifestations of the likes of Al Qaeda and the anarchist movement respectively. The next section presents this fundamental

---

[65] Stuart Shapiro, "Caught in a Web: The Implications of Ecology for Radical Symmetry in STS," *Social Epistemology* 11, no.1 (1997): 97–110.

[66] Charles W. Kegley, *International Terrorism: Characteristics, Causes, Controls* (New York: St. Martin's Press, 1990), 105.

[67] Ibid.

transformation in the sociotechnical boundaries of reality expanded into the digital world as an essential environment to consider when constructing the sociotechnical ecosystem. The contemporary social environment is now just as dependent on digital worlds as it is on the physical one.

III. EXPLORING THE CONSTRUCT OF IDENTITY

A. A PRIMER ON IDENTITY

With the intention of offering a framework to compare the technicity of an individual to the sociotechnical ecosystem (described in the previous chapter), it is important to understand that an individual's technicity is essentially her or his technological identity. This is particularly relevant in the context of social interaction and group identity because group members rely on human constructions to interact (see Figure 1). This includes the very language used by group members to exchange information to define their identity. This chapter starts with a review of classical formulations of identity and then dives into what identity is becoming in a technologically constructed reality.

"Remember when, on the Internet, nobody knew who you were?"

Figure 1. Modern Life[68]

A search of the term identity leads to abundant findings in the disciplines of anthropology, philosophy, psychology, sociology, and computer science. The broad and multidisciplinary concepts of identity often intersect but also leave unanswered gaps in the understanding of individual self-perception and behavior with respect to technological adoption. In contrast, the term sociotechnical identity does not yet appear to be a colloquial term used in contemporary sociology or philosophy. The concept of sociotechnical identity lives near the intersection of a group's hermeneutics, ingroup narrative, and the technicity of the group's environment. This chapter constructs a framework for sociotechnical identity throughout to describe the individual identity a person develops through psychological and sociological means and the evolving technicity of his or her environment.

[68] Source: "Dogs Internet" [image], Axiom, accessed October 15, 2016, http://www.acxiom.com/wp-content/uploads/2015/03/EW-dogs-internet-TCB-141508.jpg.

B. TRADITIONAL FRAMEWORKS FOR STUDYING IDENTITY

Philosophy, sociology, and psychology all answer important questions about the nature and malleability of identity, but they offer limited accounts of the influence of a technium on ascribed and avowed identities. Ideas of identity persistence have reached a critical point where on the one hand individuals can instantly alter or redefine themselves infinitely through social media by curating multiple iterations of themselves. On the other, the internet creates a nearly unalterable archive of potentially damaging and undeletable information. For example, if someone is arrested and acquitted of all charges, both records remain online but have separate search results leading to different databases and websites. The individual in question may be innocent, but the arrest record will likely feature at the top of a very visible public web search, thus upholding to the false perception of a criminal identity. Classical perspectives on identity are now fraught with these dilemmas and restructurings of the understanding of identity. Reviewing the classical frameworks provides a good starting point to explore new implications of transformative technologies on questions of identity.

1. Philosophy

In a technologically focused report entitled *The Future of Identity*, Bostrom and Sandberg provide a useful summary of the philosophical concerns with respect to identity by explaining,

> the philosophy of personal identity is a large field, but some of the key questions include whether there is a persistent identity over time, how important personal continuity is, the relation between numerical identity (being the same person) and qualitative identity (being similar to a past or future self), the links between our minds and bodies, and whether there even exists a self.[69]

These are fundamental questions to consider in light of the digitization of the self and social identity. Modernization is challenging both philosophical and homeland security scholars to understand what the nature of identity is as biometrics, genetic engineering,

[69] Ibid.

medical and sensory enhancements, robotics, and artificial intelligence develop as a human continuum and are becoming so pervasive.[70]

a. Dualism

When considering modern philosophy, the first question on identity is of course Descartes's statement "*cogito ergo sum*" (I think therefore I am), which is concerned with the duality of mind and body and suggests that identity is primordially the combination of a biological self and a soul.[71] Descartes's dualism has been criticized and called into question by other philosophers, but few conditions challenge his idea in the way augmented intelligence and genetic engineering do. If the body's building blocks can be fundamentally altered or we can teach a machine to think, then simply thinking or being are no longer enough to define oneself. Furthermore, if we consider the contemporary requirements to ascribe identity, we quickly realize that the body is not contingent. In the context of a sociotechnical professional ecosystem, for example, the identity of the individuals engaged in some activity may be entirely mediated electronically without any relevance placed on the body, yet the assumption of some authentic individual, some human, is in no way compromised.

Practically speaking, the social perception of identity is ensured without requiring the presentation of mind and body. One may question one's own essence absent mind or body, but the expectation does not seem requisite to accept the authenticity of someone else's identity. In turn, this raises questions regarding the validity of this other's identity and if it can be considered authentic if only attributed and experienced by someone else through technology mediated social interaction. Does the meaning and context of exchanged communications fulfill the *thinking* aspect of Cartesian identity, while the physical presence of emails, short messages, photos, and avatars become acceptable as a substitute to the body? Either the requirement for a body is no longer necessary or digital presentations of the self in the form of a computer-mediated social participant has

[70] Luppicini, "The Emerging Field of Technoself."

[71] René Descartes, *René Descartes: Meditations on First Philosophy: With Selections from the Objections and Replies,* ed. and trans. John Cottingham (Cambridge: Cambridge University Press, 2013), vii.

become implicitly acceptable as a substitute for the biological. Consequently, this perspective would also pave the way for the humanization of artificial intelligence, capable of passing a Turing test by making the interlocutor believe, or perhaps more significantly not care, whether she is communicating with another human.

b. Numerical and Qualitative Identity

Another fundamental philosophical split with respect to identity is between numerical identity and qualitative identity.[72] Numerical identity pertains to questions of sameness over time, or in other words, the persistence of identity as time, context, or perceptions change.[73] We can ask the question, for example, whether a child born with a strong leaning toward pacifism, who eventually is drafted to fight in war and is brought to kill the enemy, eventually changing internal perspectives on the justification of killing and on questions of death, is the same person as the innocent child he or she once was. Numerical identity implies that internal narrative and self-perception are detached from fundamental identity. It also implies that any external perception of identity, such as the projection of perceived identity by others, also bears no impact on actual identity.

The human body is also constantly being altered and transformed whether naturally or artificially. According to Frisen, a stem cell biologist at the Karolinska Institute in Stockholm, the human organism is thought to nearly fully change and regenerate all cells every seven to 10 years, pointing against a certain biological continuity and support for a physical foundation of numerical identity aside from DNA.[74] Therefore, some argue that DNA is the ultimate bearer of identity, assuming that the numerical identity of the individual remains the same. These individuals would argue that the numerical identity of the person is the same because she or she is still genetically the same. This argument is often brought up in discussions of biometric security and how

---

[72] Eric T. Olson, "Personal Identity," in *The Blackwell Guide to Philosophy of Mind*, ed. Stephen P. Stich and Ted A. Warfield, vol. 9, Blackwell Philosophy Guides (Malden, MA: Blackwell Publishing Ltd, 2003), 353.

[73] Harold Noonan and Ben Curtis, "Identity," *Stanford Encyclopedia of Philosophy*, April 25, 2014, http://plato.stanford.edu/entries/identity/.

[74] Nicholas Wade, "Your Body Is Younger Than You Think," *The New York Times*, August 2, 2005, http://www.nytimes.com/2005/08/02/science/your-body-is-younger-than-you-think.html.

easy it is to manipulate fingerprints, retinas, and other physical characteristics opposed to the complex and unique sequence of DNA. However, the ability to clone, reproduce, and modify genes through genetic enhancements are already technologically available. If the argument that DNA confers the ultimate identity designation is supported, then would not any exact reproduction of DNA be the identical numerical DNA? Would an exact clone be the same identical person? Would someone with altered DNA become someone else? From a criminological perspective, if a legal system is based on numerical identity and attributes some governmental identification number for life, would genetic alteration of the individual's natural DNA still confine the person's identity to the same numerical identity? So, can someone alter his or her fundamental identity through various technological means? What is certain is that the biological and cognitive definitions of individual identity are changing, leaving the fundamental principle of identity unclear. This has direct consequences on social identity as individuals, cast as members of an outgroup based on ascribed characteristics, have the capacity to alter or abandon them for ingroup characteristics.

On the other hand, qualitative identity holds that the fundamental identity of an individual changes over time and that an adult with a certain knowledge set and experience is not the same person as a former self.[75] Qualitative identity roots itself in the continuity of a closely similar being to a past iteration and a future self.[76] This perspective has very important implications in the context of sociotechnical identity because as humanity continues to move toward increasing technological embodiment and greater human-machine integration, the possible iterations of new and transformed qualitative identities are taking unprecedented shapes. This is particularly true when it comes to the definition of self-identity shaped by the perception of one's reality, a space coined *umwelt* by German biologist Jakob von Uexküll in 1909.[77] In contrast to the sensorially shaped reality is the concept of *umgebung*, which accounts for the rest of the

[75] Nick Bostrom and Anders Sandberg, *The Future of Identity* (London: Future of Humanity Institute, Oxford University, 2011), http://www.nickbostrom.com/views/identity.pdf.

[76] Noonan and Curtis, "Identity."

[77] Nieto-Gómez, "This Is Your Brain on Code."

physical reality or surroundings that go imperceptible to an organism.[78] The composition of umwelt and umgebung are different for different organisms and for individuals with varying sensory capacities. For example, the subjective experience of reality will be different for someone who is deaf, blind, or with tactile insensitivity as compared to someone with intact senses. Emerging technologies though are facilitating and improving synesthesia, the body's ability to perceive a sense through the stimulation of another sense. By absolving human sensory system degradation from aging or behavior through artificial augmented, the boundaries of the human umwelt are shifting. In "This is Your Brain on Code: Embodied Intelligence Augmentation and Conflict," Rodrigo Nieto-Gomez uses the example of cochlear implants, the first artificial sensory receptors, to demonstrate how technology is altering the human umwelt and therefore playing an undeniable role in shifting identity.[79] With the umwelt denoting the "subjectively perceived surroundings about which information is available to organism through its senses,"[80] the implication that reality is subject to an organism's senses reaffirms that contemporary and future reality will largely be defined by technology, rather than just socially constructed as proposed by Berger and Luckmann.[81] This is an important matter for homeland security forecasting because as technology enables the transformation of people's umwelt, inevitable grievances will begin to emerge raising ethical questions regarding human rights and the capacity to pursue biotechnical enhancements.

2. Sociological Perspectives on Identity

Sociological perspectives on identity tend to fall into two dominant schools: *identity theory* and *social identity theory*. Abrams and Hogg define social identity as "a

[78] David Eagleman, "The Umwelt," *David Eagleman* (blog), 2012, http://www.eagleman.com/blog/umwelt.

[79] Nieto Gómez, "This Is Your Brain on Code."

[80] Kari Lagerspetz, "Jakob von Uexküll and the Origins of Cybernetics," *Semiotica* 134, no. 1/4 (2001): 643–651.

[81] Jui-Pi Chien, "Umwelt, Milieu (X), and Environment: A Survey of Cross-cultural Concept Mutations," *Semiotica* 2007 no. 167 (2007): http://philpapers.org/rec/CHIUMA, 67.

person's knowledge that he or she belongs to a social category or group"[82] as a process of self-categorization, while *identity theory* considers the same process, which it names *identification,* to be dependent on "a named and classified world [in which] the core of identity is in the categorization of the self as an occupant of a role, and the incorporation, into the self, of the meanings and expectations associated with that role and its performance."[83] Either way, what remains a fundamental commonality of these theories is that individuals "view themselves in terms of meanings imparted by a structured society."[84] This is of great importance to a discussion about technology because the organization of a society is itself a technological construct. It is the product of an imagined order, created by humans, used to manage or maintain access to resources. Thus, identity in the sociological context is fundamentally dependent on a technology: an organized system of networked individuals. Therefore, social structuring needs to be considered part of the technicity of sociotechnical ecosystems, and I use the term *network structure* to describe it.

3. The Asymmetry of Personal and Social Identity

If the assumption that identity is some product of multiple layers of ascribed and avowed identity designators such as age, gender, sexuality, ethnicity, profession, religious affiliation, interests, and others is correct, then a distinction between individual and group identity immediately emerges. Individual identity is composed of many layers of ascribed and avowed identities, while social identity is essentially constructed of only several avowed designators. What this means is that the complexity of individual identity exceeds that of group identity, which is usually forged around a common interest, purpose, or imperative. This could partially explain the phenomenon of groupthink,

---

[82] Dominic Abrams, and Michael A. Hogg. "Comments on the Motivational Status of Self-Esteem in Social Identity and Intergroup Discrimination," *European Journal of Social Psychology* 18, no. 4 (1988): 317–334.

[83] Originally from Dominic Abrams and Michael A. Hogg, "Comments on the Motivational Status of Self-Esteem in Social Identity and Intergroup Discrimination," *European Journal of Social Psychology* 18, no. 4 (1988): 317–334, http://onlinelibrary.wiley.com/doi/10.1002/ejsp.2420180403/abstract, quoted in Jan Stets and Perter Burke, "Identity Theory and Social Identity Theory," *Social Psychology Quarterly* 63, no. 3 (2000): 224–237, http://wat2146.ucr.edu/papers/00a.pdf.

[84] Stets and Burke, "Identity Theory and Social Identity Theory."

which consistently seems to be inferior to personal judgment, or conversely, the difficulty some individuals have at overcoming an overabundance of choices. Without the ability to simplify personal identity through social categorization, it is likely that an individual's identity would be more susceptible to internal contradiction or disruption than that of a standard group, since there are more superimposed layers that can contradict themselves. For instance, much of the discussion on radicalization has come to focus around the issue of conflicting identities and how many disaffected youth find themselves seeking an ideal community to belong to. The issue that emerges is that individuals with complex and opposing identity characteristics, including some of the very characteristics that groups adopt to define their own social identity, end up rejected by either ingroup. This sociotechnical disaffection leads to

> immigrants who identify with neither their heritage culture nor the culture they are living in [feeling] marginalized and insignificant. Experiences of discrimination make the situation worse and lead to greater support for radicalism, which promises a sense of meaning and life purpose.[85]

According to social identity theory, individuals

> maximize the differences between the ingroup and the outgroup (it is necessary to maintain that the groups are distinct if a person is favoring their group over the other) [and] minimize the perception of differences between ingroup members (this increases ingroup cohesion).[86]

This means that individuals reduce their social identity to a few strong ingroup markers while the formation of individual identity, just like intergroup comparisons, tends to maximize differences from their environment in the process of their social categorization. As a result, individuals are subject to complex nominal identities that drive them to seek social belonging as a solution to a more manageable sense of individual identity. This reduces the need to orchestrate potentially conflicting identity markers by abandoning aspects of the self to a collective bargain on identity. This necessity was described in other terms in Maslow's hierarchy of needs as the stages of *belongin*g and *esteem*

[85] Sarah Lyons-Padilla et al., "Belonging Nowhere: Marginalization and Radicalization Risk among Muslim Immigrants," *Behavioral Science & Policy* 1, no. 2 (2015): 1–12.

[86] "Social Identity Theory (Tajfel, Turner)," Learning Theories, December 15, 2015, https://www.learning-theories.com/social-identity-theory-tajfel-turner.html.

whereby individuals gain footing in their sense of self though the reflection of others.[87] While social structures and networks are a human device to coalesce multiple individuals around similar identity markers, the participants' social identity becomes in turn technologically defined and therefore imparts a sociotechnical identity on all members.

We can see a correlation emerging between the number of identity markers an entity has and the strength of its sense of self. It is understood that a group is composed of individuals who all bring a complex amalgamation of individual identity designators, but a strong ingroup narrative is generally defined by maybe only one, two, or three avowed factors. In strong social groups, many if not most of the individual ascribed identity markers of a group's members play no part in the collective identity. For example, the U.S. Senate as a group is composed of U.S. citizens, elected by the people to fulfill duties and responsibilities granted by the Constitution. These three parameters impart the identity designation of senator. The group identity of the Senate is not constructed or constrained by gender, ethnicity, sexual preference, ancestry, dietary constraints, or any other deeply individual identity marker. As another example, the Hell's Angels, who are a sociotechnical group with a strongly held collective identity made up of an artifact facilitating mobility, Harley-Davidson motorcycles, and a network structure organized around gender and race, notably white males.[88] This points to the fact that the defined identity of a group lacks the quantitative complexity and depth of the individual identity schema but makes the shared group markers assimilated with more prevalence. The individual prioritization of a group identity marker over the selection of individual markers is also supported by Maslow's hierarchy of needs, whereby the pursuit of social approval and social belonging precedes the pursuit of self-esteem and self-confidence.[89]

---

[87] Mark E. Koltko-Rivera, "Rediscovering the Later Version of Maslow's Hierarchy of Needs: Self-Transcendence and Opportunities for Theory, Research, and Unification," *Review of General Psychology* 10, no. 4 (2006): 302–317.

[88] *Wikipedia*, s.v. "Hells Angels," November 10, 2016, https://en.wikipedia.org/w/index.php?title=Hells_Angels&oldid=748836305.

[89] Abraham Maslow, "A Theory of Human Motivation," *Psychological Review* 50, no. 4 (1943): 370.

This description of identity does not make a qualitative assessment or attribution of value to either social or personal identity but simply tries to point to the difference in the multiplicity of accepted values defining the whole. If the assumption that personal identity is composed of more variables than group identity is correct, then it is reasonable to assume that an ingroup narrative is also subject to less internal contradiction and therefore a more stable identity marker for any given group. Practically speaking, this means that it would be much easier to recruit and convince an individual to join a terrorist group or fight for a cause that may not originally be his or her very own than it would be to convince a group like a drug cartel to abandon the drug trade for some other business model or for Al-Qaeda to give up on fighting Western interests through unconventional means. In other words, individuals are often more likely to defer or abandon their own definitions of identity than they are to abandon the group markers that they adopt as their own. This supports a logical explanation for suicide bombers who favor their identity as a member of a group over their individual identity up to death itself. This difference may raise questions about the strength of an identity iteration for any particular individual and seems to divide attributed identity from assimilated identity. There are differences in importance and perceived authenticity between the markers of identity imposed on an individual, such as being of a specific gender, born into a certain nationality to parents of a certain religion and economic status, and factors that are subsequently chosen throughout personal development to define the self-constructed identity, which seems entirely constructed of sociological and technological experiences. The reason for understanding this difference becomes even more important when the only social ingroup that an individual has to deal with is either through remote communication tools or with an unknowingly digitally fabricated social ingroup of online avatars or trolls. This presents one of the critically dangerous boundaries of sociotechnical ecosystems and is further explored in a later section.

When focusing on the context of homeland security and more specifically on terrorism analysis, social identity theory offers a useful lens of four specific analytical markers to understand “a group’s behaviors and relationships to other groups [...] by examining both its social context and its members’ understanding of themselves and their

group within that context."[90] The framework helps overcome preconceived notions and cognitive and emotional biases in analysis by requiring great attention to be placed on context, culture, and ideology.[91]

The analytical markers used in social identity theory are "patterns of patron-client relationships, interactions centered on the acquisition of honor and avoidance of shame, perceptions of a 'limited good,' and behaviors of "challenge and response."[92] This approach to studying terrorism and intergroup conflict uses a deeply sociological terminology to describe and define the dynamics at play within and between social groups. Implicit in these analytical markers are elements of social technicity, which without overt statement can be overlooked or neglected as playing an important role in influencing group behavior. Furthermore, as described in the second chapter, the emerging technological paradigm exerts a growing influence on social behavior in subtle and often imperceptible ways. While social identity theory proposes that identity is a matter of how individuals categorize themselves within the social context, shifting and evolving technologies also entrain people's perceptions of self and in turn lead them to behave in response to forces of which they may not be aware. For example, the rapid expansion of social media platforms has led to real-time global exchanges on blogs and in forums through media outlets with disregard for geographic or political boundaries, thus altering the frequency of the challenge and response cycle. This has also led to a growing feeling of a globalized self, allowing the world to feel "closer" and the development of a single interdependent economic system.[93] Traditional ingroup-outgroup divides, such as nationality, religion, gender, or age, are giving way to more ingroups formed around common interests, customized worldviews, and fragmented individual characteristics.

---

[90] Brannan, Darken, and Strindberg, *A Practitioner's Way Forward*, 47.

[91] Ibid.

[92] Ibid., 65.

[93] Ray Barrell and Tatiana Fic, "Integration, Globalisation, Technology and Trade Patterns in the EU8," *Research in Economics and Business: Central and Eastern Europe* 2, no. 1 (2013): 34–46, http://rebcee.eu/index.php/REB/article/view/23, quoted in "The Influence of Modern Technology on Society," UKEssays, accessed December 10, 2016, https://www.ukessays.com/essays/social-policy/the-influence-of-modern-technology.php.

Specific technologies, such as mobile devices like smartphones, which have grasped the near constant attention of many users and distract them from significant face-to-face social interactions, are also promoting behavioral change. Their use, which allows adopters to spend their time in online social relationships and interactions rather than physical ones, is also undermining social connection and empathy. This phenomenon is aptly identified in "The Empathy Paradox: Increasing Disconnection in the Age of Increasing Connection," in which Sara Konrath writes, "this new media landscape could lead to increasing social disconnection even as it superficially increases our social connections, and several studies suggest a direct link between social media use and social disconnection."[94] This paradox is further explored in the next chapter in which the idea of a growing non-human social paradigm is proposed. The age of interconnection is also becoming an age of individualism, which may undermine the strength of ingroup cohesion in the face of conflict. The modern business space may offer a good example as frequent criticism of the so-called millennial generation highlights a high turnover rate in young employees faced with mild confrontation or dissatisfaction with their peers.[95]

Social media is also leading to the reshaping of network structures and favors a scale-free social arrangement, moving away from traditional vertical hierarchies, which have shaped social identity perspectives as implied by the patron-client relationship structure of social identity theory. The value of social identity theory as a framework is not in question; however, the need for some room for a refinement in the analysis of terrorism is growing, and consideration for a sociotechnical ecosystem perspective may help fill that gap.

[94] Sara Konrath, "The Empathy Paradox: Increasing Disconnection in the Age of Increasing Connection," in *Handbook of Research on Technoself*, ed. Rocci Luppicini, 204–228 (Hershey, PA: IGI Global, 2012).

[95] "Attention, Employers: Millennials Have Made Their Demands," *The Atlantic*, accessed January 15, 2017, http://www.theatlantic.com/sponsored/allstate/attention-employers-millennials-have-made-their-demands/219/.

C. THE TECHNOSELF—AN INTERFACE ONTOLOGY OF THE EXPERIENCE OF IDENTITY AND TECHNOLOGY

Online identity is self-defined on social media accounts like Facebook or LinkedIn, which people use to curate personal and professional identities. Personal identities may also be shaped by others who attribute values through comments or ratings as with sites like RateMyProfessor.com wherein students generate ratings and influence social perceptions of college professors beyond professors' direct control. Finally, online identity may represent a completely invented persona living a full digital life with falsified socioeconomic characteristics and free from the material limitations of a physical body. The ability for people who are unpleased with their authentic identities to recreate themselves online to their own liking, while maintaining their physical identities anonymous, is changing the importance and perceived authenticity of the virtual identity.

1. The Virtual Self

The increasing number and types of options for digital self-presentation are creating an interesting set of phenomena in terms of social interaction and human experience. McCreery studied participants' phenomenological personality and presence after playing massively multiplayer online games (MMOGs) to evaluate the symmetry and differences between physical and virtual selves. The research confirmed prior assumptions that the human experience, defined as social by nature, extended beyond physical spaces and particularly in virtual space.[96] The conclusions drawn echo and cite the works of Pavel Curtis and Christian Bessiere regarding the psychological connections and possessiveness to one's avatar characters.[97] Although much more research is necessary to understand the full psychological and behavioral influence avatars and computer-mediated environments exert back onto their participants, two interesting observations with potentially direct homeland security impacts from psychological and behavioral changes have already been made regarding self-projection into virtual spaces.

[96] Michael Patrick McCreery, "Personality, Presence, and the Virtual Self: A Five-factor Model Approach to Behavioral Analysis within a Virtual Environment," (PhD diss., University of Nevada, 2011), http://digitalscholarship.unlv.edu/thesesdissertations/1043.

[97] Ibid.

First, the development of online addiction to "cyberdelics" point to potentially dangerous alterations in self-perceived identity and physical behaviors when the psychological attachment to avatars becomes an authentic experience. The concept of " cyberdelics, most recently written about by Rushkoff in *Cyberia*, surfaced after the LSD enhanced hippie movement as a computer mediated counter-culture, which has arguably led to the cyberpunk, cypherpunk, and hacker cultures, and I would argue, most recently, to the post-factualism movement.[98] While the use of LSD, popularized in the 1960s, manipulated the internal biochemical environment of the human body to generate hallucinations, giving the user an altered sensory experience of an imagined hyperreality, the development of cyber technologies allows users to immerse themselves in a computer-mediated virtual reality in which the senses function appropriately but deliver an artificial hyperreality akin to a hallucination. Therefore, it should be noted that when the users become distracted enough by the sensory input of their experience to forget that it is being technologically reconstructed, they lose the ability to discern fact from fiction and may be compelled to modify their behavior according to that perceived sociotechnical construct of reality. This becomes concerning when "cyberdelics" are designed to drive social identity toward violence or hatred and result in criminal or terrorist acts rooted in a form of sociotechnical hallucination.

Second, the concept of *digiphrenia*, introduced by Douglas Rushkoff in the book *Present Shock: Where Everything Happens Now*, is defined as

> the experience of trying to exist in more than one incarnation of yourself at the same time. There's your Twitter profile, your Facebook profile, your email inbox. [...] All of these sort of multiple instances of you are operating simultaneously and in parallel. And that's not a really comfortable position for most human beings.[99]

This observation underlines a contemporary tendency in many information technology users to lose any tight sense of self-identity or prevalent social identity as a result of

[98] 92Y Plus, "Brain Jazz: A Mind-Jam with Jason Silva and Douglas Rushkoff," YouTube, January 2, 2014, https://www.youtube.com/watch?v=HTP0NQlyB3w.

[99] Douglas Rushkoff, "In a World That's Always on, We Are Trapped in the 'Present,'" interview by Audie Cornish, *All Things Considered*, NPR, March 25, 2015, http://www.npr.org/2013/03/25/175056313/in-a-world-thats-always-on-we-are-trapped-in-the-present?sc=ipad&f=1019.

developing and curating multiple online personalities. This also implies that as a result of conflicting self-identities, individual dedication to any single social narrative is likely to be strongly undermined by technological factors. Consequently, we can conclude that emerging technologies undermine what we currently understand of social identity and the effectiveness of social identity theory.

McCreery wrote, "it is clear the avatar is no longer a caricature but an emerging virtual self," yet it is replete with improvisations, imagination, and transgressions of reality.[100] These transgressions have become an acceptable part of how we define ourselves to others, and in turn, we have become more accepting of the transgression of truth from information permeating out of computer-mediated environments, including the contemporary media stream. The development and identification of these virtual-self pathologies expose the susceptibility of certain individuals to adopting and joining virtual social representations of counterculture groups despite having no affinity for real-world participation in fringe groups or law breaking.

Concretely, the growth of the individual self-projection into cyberspace solidifies the dependence and response to information within that same system. In turn, this means that engineered computer-mediated technologies can in certain cases be used to recruit or control individuals with at least as great a degree of success as traditional in person recruitment, indoctrination, or coercive methods normally used in physical contexts and described by social identity theory.

2. Synthetic Communities

According to Rheingold, virtual communities are "social aggregations that emerge from the Internet when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace"[101] It is generally agreed that individuals using social media and the Internet of Things (IoT) for either communication or self-curation develop a virtual self. It follows that those same

[100] Ibid.

[101] Ana-Cristina Ionescu, "Cyber Identity: Our Alter-Ego?," in *Handbook of Research on Technoself*, ed. Rocci Luppicini, 190–203 (Hershey, PA: IGI Global, 2012).

individuals build a tolerance for interaction with the virtual other. Any rejection of a sense of authenticity in other virtual personas found online would undermine the sense of authenticity of one's own personal virtual self. This adds to the digiphrenia and has the effect of ultimately diluting the value and importance of transparent and honest human exchange. The machine interlocutor eventually becomes wholly legitimate, as demonstrated by Apple's Siri when a question is answered and immediately accepted as fact. This phenomenon has generated a countless global virtual population of trillions of influential avatars undermining the guarantee and subsequently the expectation that another human sits behind the screen. This undermines human accountability, a dissuasive force against malicious acts enforced by judicial systems, because it is difficult to attribute guilt when an anonymously controlled avatar is to blame for an individual's radicalization.

This encounter of virtual people, unconstrained by the traditional physical and social limits of biological reality, becomes a metaphorical representation of identity and personality traits. This creates a significant concern for homeland security because large segments of the population are becoming more receptive and responsive to virtual personas of unknown origin or identity with whom they build up relationships and even go as far as physically obeying their ques. Social identity theory talks of *patron-client* relationships as an important marker of social construction, but as artificial intelligence grows, we are beginning to see the introduction of anthropomorphized information technologies and algorithms interacting with humans and integrating these traditionally human *patron-client relationships*. This provides a simple example of the interplay of technology on traditionally human behavioral systems and understanding.

The recruitment of western youth through online personas, inviting them to travel to Syria or Iraq to join ISIS in jihad, demonstrates the degree of trust that can be placed in an avatar. The real threat is that as artificial intelligence continues to improve, an army of avatar recruiters could be programmed to tailor their recruitment strategies through machine learning to the most vulnerable targets, resulting in larger numbers of radicalized individuals.

The interaction between a person and a computer mediated avatar is a metaphorical experience of some dimension of human identity. The appeal of engagement with these characters or computer-mediated personas might be better understood through the work of Ramachandran and Hirstein. In "The Science of Art: a Neurological Theory of Aesthetic Experience," they offer a perspective on the effect and appeal of metaphors on the brain.[102] A metaphor creates a feeling of synesthesia in the brain by developing a sense and feeling of discovery, which is subsequently rewarded by a surge of dopamine. This elicits an appealing satisfaction and, in some cases, initiates a dependency or addiction to the specific input in question, which in this case is the interaction with computer-mediated personas. The more elaborate and refined the experience of the virtual identity becomes, usually enhanced through personality similarities and lifelike characteristics, the stronger the synesthetic effect and eventual acceptance of a new umwelt.

These changes in technology and sociotechnical ecosystems simulate the experience of a sensory form of reality and consequently drive the user to adopt the new contextual social identity, one which may be devoid of any direct human interaction. This example partly frames the development of the concept of sociotechnical identity. While discussions involving the future of mankind as a technological being focus predominantly on the direct integration of humans and technology and the subsequent impacts on a larger society, we might be missing the important point that individuals are deriving their social experiences and integration to so-called ingroups through machine organized and controlled experiences—in other words, sociotechnical ingroups.

While much media attention is placed on humans transitioning toward cyborgs, individuals' synthetic social groups are slowly divesting themselves of human participants and turning unnoticed into inorganic structures powered by artificial intelligence and machine learning. This means that a social ingroup can now be entirely formed by virtual representations of humans, such as bots, designed and tailored for

[102] Vilayanur Ramachandran and William Hirstein, "The Science of Art: A Neurological Theory of Aesthetic Experience," *Journal of Consciousness Studies* 6, no. 6–7 (1999): 15–51, http://www.ingentaconnect.com/content/imp/jcs/1999/00000006/F0020006/949.

maximal appeal or propaganda purposes. Homeland security may already be facing its very first war against the machines, not by fighting technology directly but by contending with people reacting and responding to the influence of their own cyber umwelt. This understanding may be a key component to combating the successful recruitment and radicalization of a technologically dependent generation with fluid perspectives on their social purpose and identity.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A FRAMEWORK TO EVALUATE THE TECHNOSOCIAL CONTINUUM

Up to this point, we have surveyed the various perspectives and theories on the interaction of society and technology and how contemporary innovations in cyber technologies and the technium are driving human engagement, self-identity, and a shift from social identity to sociotechnical identity. Given this inextricable influence, the technium has been determined to play in shaping identity, and it is essential to try and define the boundaries or dimensions of the superposition of the social experience and the technium.

This chapter uses a military example to construct a sociotechnical scaffolding of identity around the technicity of a soldier. The framework as a whole is referred to as a *sociotechnical ecosystem*, and it has been developed to provide an encompassing methodology for considering how the interface of social groups and technology influence human behavior and build specific definitions of identity. The next section uses the U.S. military's definition of a soldier as an ontological example of a sociotechnical ecosystem and is used to define five domains of sociological technicity. These domains eventually set the boundaries of sociotechnical ecosystems.

A. A SOCIOTECHNICAL ECOSYSTEM MATRIX

This section uses the functional responsibilities of soldiers in the U.S. Army, as well as the organizational necessities of a military organization, to develop an ontological framework of sociotechnical ecosystems. The goal is to extract a taxonomy of the fundamental dimensions of the technium that are socially interdependent. This offers an opportunity to think about how a group may adopt new technologies or how emerging technologies may transform group dynamics. The proposed framework follows an exercise in ontological engineering in an attempt to simply frame the boundaries of social context in a technologically dependent environment.

The "Army Warrior Tasks" as defined by the U.S. Army Training and Doctrine Command states that soldiers, who can be considered as sociotechnical beings, need to

"shoot, move, communicate, survive, and adapt while operating in the contemporary operational environment."[103] The first three of these explicit tasks (shoot, move, communicate) are sociotechnically dependent dimension of the soldier's mission, which I suggest renaming *artifact*, *mobility*, and *communication*. The ability of soldiers to shoot at the correct target is dependent on the possession of physical objects or *artifacts* of war, notably weapons, armor, and uniforms. Their ability to move is dependent on a complex combination of factors, including terrain selection, a capacity to overcome obstacles, physical displacement, vehicles, formations, or confinement, which are all aspects of the technicity of movement or *mobility*. Lastly, soldiers need to define goals and objectives, to coordinate operations, to exchange information with a common language and terminology, and to build rapports of trust through *communication*.

An observation that immediately emerges from these preliminary categories is that they are all also highly interdependent. For example, the mobility of soldiers is dependent on artifacts, such as aircraft and ships, which use communications to coordinate traffic in dense areas. Those very communications are also dependent on artifacts, which have been engineered to function for mobility, such as radios for talking remotely, smoke signals for geographic marking, or lasers for targeting. Further observations of the selected example immediately point to a functional continuity between the technological dimensions listed. For instance, using two-way radio communication, something many would consider an improvement in communication technology, is in actuality a re-engineering of the sociotechnical dimension of mobility applied to a group's capacity to communicate. The two-way radio as an artifact was indeed an improvement in communication technology, but sociologically it transformed group mobility more than anything.

Continuing with the stated soldier tasks, as with any dynamic environment, both natural and technological, there is a constant need to evolve over time. In this context, it is fueled by the imperatives of *survival* and *adaptation* in the sociotechnical environment

[103] U.S. Department of the Army, *Basic Officer Leader Training Policies and Administration* (TRADOC Regulation 350-36) (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2015), http://www.tradoc.army.mil/tpubs/regs/TR350-36.pdf.

of war. Survival and adaptation, identified here as key tasks for all soldiers, need to be recognized as important conditions of change over time in any sociotechnical ecosystem. While these do not form a dimensional category of sociotechnical ecosystems, they help orient the decision scheme in technicity adoption and change over time. In other words, social groups are compelled toward technological adoption for both survival of the group and adaptation to its environment. In the military context, this manifests as the pursuit of constant innovation in weaponry and in strategy to outperform other militaries. This is the same in any private sector environment in which businesses are forced to constantly innovate their products, their organizational management, and their vision or else fail under the pressure of competition.

In addition to the explicit tasks discussed, there are also implicit factors framing the warrior ecosystem that require an understanding of the legal and organizational construct of militaries allowing the soldiers to carry out their actions. For soldiers to exist, they must be legally defined and constrained by a body of law. Their authority must be established and constrained by leaders, policies, and in certain systems by public will. Lacking this legal authority to wage war could lead an entity to be denoted as a terrorist or insurgent organization.

In terms of tactics and operations, soldiers need to be assigned a place within a hierarchical network and become specialized to accomplish specific and achievable tasks. These features all pertain to network structures as the technological dimension for quantitatively and qualitatively classifying human function and identity. As social groups shape themselves, they can assume any variety of network configurations. Face-to-face networks often have a tendency to elicit competition and *patron-client* relationships and thus emerge as hierarchies. When thinking of traditional business environments, it is evident that vertical structures develop and yield control and authority to some over others. These are typified by the executive, managerial, and operational staffing layers of nearly all corporations. In online networks and social media, the network distribution is more horizontal and organizes itself into scale free networks, as discussed previously. The network organizes itself around individuals, or nodes, who are more interconnected

than others, without the platform conferring any special authority to those users.[104] For example, *Wikipedia* yields no authority to one contributor over another, and while one contributor may provide better information than another, the network remains democratized. It is also important to note that there is a network structure beyond the geometric configurations of vertical, horizontal, distributed, open, and closed networks and that it can hold a functional configuration. Examples of these are information, professional, recreational, and technological networks.

Focusing on our example, the military also depends on a knowledge base for strategy and tactics as well as means of exchange to obtain necessary tools and resources. These are technologically categorized as *information*. This category may be the most difficult to conceptualize because of the divergence of its components and its immaterial nature, but it generally represents the conceptual, data, or coding capacity of a system. The process of harnessing a natural phenomenon into a technology to achieve an unnatural outcome is dependent on the development of information as a means to regulate or hack phenomena. This pertains to the ability to concentrate energy and develop methodologies and immaterial value available within the system to reallocate it in an unnatural, concentrated, or asynchronous way. Some examples of sociotechnical information include the deconstruction of phenomena through observation and research; the development of methodologies, such as economics, political science, healthcare or education; the use and development of standardized methods of sensing or measuring and translating phenomena into data. Information can to a certain extent be thought of as immaterial artifact.

As discussed, the sociotechnical dimensions just identified are highly codependent and can be developed to substitute for or adapt to another dimension's purpose. For example, the internet, which is fundamentally a communication network technology, has substituted for mobility, artifacts, nonverbal communication, and so on. The need to travel to a brick-and-mortar bank has been eliminated by facilitating online banking. This transformation also requires the monetary artifact of currency to be

[104] Ted G. Lewis, *Book of Extremes: Why the 21st Century Isn't Like the 20th Century* (New York: Springer International Publishing, 2014), 60.

transformed into digital bytes or information for exchange. It is this technological translation from one domain to another, while still fulfilling a similar functional outcome that characterizes technological adaptation and innovation in the sociotechnical ecosystem. These systems can also be developed with very specific dimensional boundaries to contend with undesirable identity features. This is an important fact to consider when thinking about how to disrupt criminal organizations, terrorist groups, and the like.

Looking back to Arthur's definition of technology as combinatorial and recursive, we can see that the technicity of the military ecosystems also seems recombinant.[105] If this holds true, then sociotechnical ecosystems are also a combinatorial product of all their technical domains. This means that if the ecosystem evolves as a combination of recursive technological adaptations, then each of the five domains could be adapted to compensate for any limited capacity of another domain to provide a technical advantage. For example, if people's mobility is limited by the length of a telephone cord, then by modifying that artifact into a wireless phone, there will be an increase in people's travel range, or in other words their mobility. Likewise, if open communication or free speech is jeopardized by the censorship of information, then the alteration of network structures through participant anonymization and the creation of new communication platforms, such as 4chan, emerge as an adapted ecosystem to overcome the constraints on free speech. This process is elaborated upon in Chapter V, looking at how ISIS has excelled as a Salafi-jihadist contemporary of Al-Qaeda by adapting to the sociotechnical constraints placed on the later and leveraging new technologies to drive recruitment into new identity pools. ISIS has derived a new sociotechnical ecosystem through adaptation to survive the counterterrorism strategies overcoming Al-Qaeda.

If pressure is placed on one particular dimension, say the need for secrecy of information as is the case with intelligence work, the social response is to devise communication tools, artifacts, and covert relationships that mimic a different sociotechnical ecosystem and act out different social identities. Certain sociotechnical

[105] Arthur, *The Nature of Technology*, 27–39.

ecosystems, such as prisons, aim to disrupt the challenge-response cycle and develop with the specific purpose of limiting mobility as a means to correct unwanted social behaviors. By incarcerating individuals into a specific type of technological structure built around the control of mobility, communication, limiting access to information and artifacts while assigning a position of subjugation in a network structure of guards and inmates, the judicial system aims to alter criminals' avowed identity by placing them in a designed sociotechnical ecosystem, stripping away those avowed identities, and ascribing those individuals a new identity. To summarize, the five sociotechnical dimensions extrapolated from the soldier example are listed below and have been assembled into a graphic representation for the sociotechnical ecosystem (see Figure 2).

1. Artifact (e.g., tools, art/symbols, weapons, clothing)
2. Mobility (e.g., vehicles, roads, hubs, agility, social mobility)
3. Communication (e.g., language, writing, social media)
4. Information (e.g., exchange, data, software, force multiplication, processes, subject matter, knowledge base)
5. Network structures (e.g., open versus closed, vertical versus leaderless versus scale free, social, professional, informational, recreational, educational, indebted and academic).

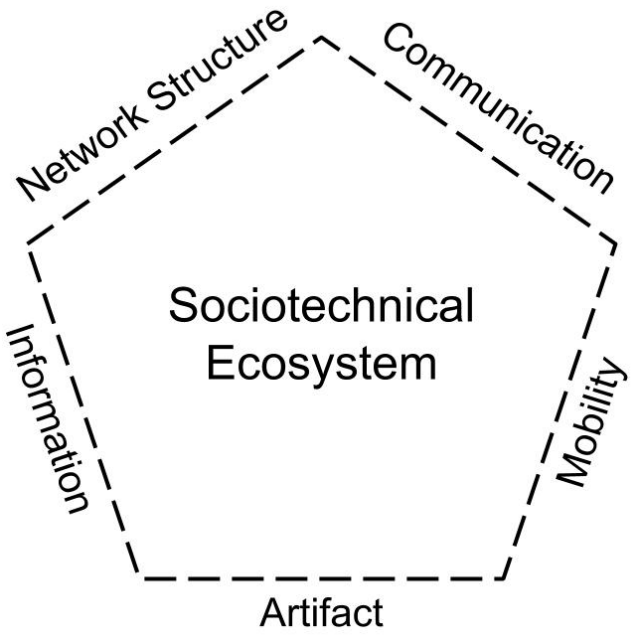

Figure 2. The Sociotechnical Ecosystem

B. SOCIAL IDENTITY THEORY IN A SOCIOTECHNICALLY CONSTRUCTED REALITY

The social identity theory (SIT) framework frequently used to evaluate intergroup conflict uses four steps each following a dialectic frame. These are defining ingroups and outgroups, patron-client relationships, identifying limited goods, and a challenge and response cycle.[106] However, once these overarching classifications of social dynamics are defined and an analyst is invited to conduct an exercise in thought regarding how social groups interact within these frames, the responsibility sits with the analyst to select and make sense of which forces to explore. There does not seem to be a methodology or framework within SIT to account for the impact on identity of an immersive technium. Having emphasized the deeply sociotechnical nature of society and the social and technical definition of "self," it may seem useful to move through the steps of SIT using the elements of sociotechnical ecosystems as a systematic process to capture and consider all important dimensions of the individual and social groups for a more comprehensive understanding of intergroup and intragroup dynamics.

[106] Brannan, Darken, and Strindberg, *A Practitioner's Way Forward*.

Following the review of literature and hypothesis for a sociotechnical ecosystem, there are three important findings that have emerged regarding sociotechnical ecosystems. First, sociotechnical ecosystems drive self-categorization and the construction of reality for social ingroups according to a system of technological dimensions. In that sense, building on the title of Berger and Luckmann's work, it could be said that reality is sociotechnically constructed.[107] Although the language used in their *Social Construction of Reality* did not exclude technicity as an implicit force influencing the perception of reality, the distinction proposed here triggers particular attention to be placed on technology itself as a continuum of the human experience.

Next, sociotechnical ecosystems need to survive internal change and need to innovate to adapt to external forces. These imperatives are expressed in SIT as the external pressures of a *challenge-response cycle* with regard to limited goods and the internal pressure of *patron-client relationships* that shape into the *network structure* dimension of an ingroup.

Finally, the strength of a group's social identity, in other words their cohesiveness, is derived by their ecosystem and is related to the level of interdependence of the technological dimensions of that ecosystem. For instance, a mobile phone is a high order technology because it is a physical artifact that allows multiple forms of communications, facilitates physical and cyber mobility, provides information to aid in navigation and computation orders of magnitude above human capabilities, and imparts a certain social status or label, such as Millennials. In that sense, members of a group that have adopted mobile technology as a preferred resource are more adaptive to their environment but are also more vulnerable targets to disruption because the elimination of their mobile devices would leave them deprived of several sociotechnical dimensions. A toothpick as an example of a simple technology, has a single intended purpose as an artifact, and therefore provides limited intrinsic social cohesion. Gradually, all technologies evolve to adapt to emerging social needs or constraints and carve out new categories of identity.

[107] Berger and Luckmann, *The Social Construction of Reality*.

This technological evolution, which Brian, Kelly, Ellul, and others have described, is carried out by human catalysts actualizing a simultaneous cooperative and competitive materialization of new constructed ecosystems and realities. In this sense, technology can be thought of a complex exomorphic extension of humanity. Like a limb and through a form of synesthesia, it allows its user to discover and pursue new subjective experiences. The idea of a technoself, as promoted by Luppicini,[108] provides a method to explore human phenotypes within an evolving definition of reality. Comparing an individual's technoself to a sociotechnical ecosystem can provide insight into future internal motivations of that individual. If that individual is already a key member of an ingroup, then their technoself may suggest the likelihood of the ingroup to shift and adapt its technological use or it may provide insight into the allegiance and propensity of the individual to defect from the group. These all provide important intelligence, investigative, academic, and economic insights that fall within the homeland security prerogative.

To help with the operationalization of this concept, the sociotechnical ecosystem can be thought of as a system of five functions or a type of coordinate system where network structures, information, artifacts, mobility, and communication function as axes upon which the technological adoption, adaptation, and use by individuals can be evaluated to provide a snapshot of a group's technicity and thus sociotechnical identity.

[108] Luppicini, *The Emerging Field of Technoself Studies.*

THIS PAGE INTENTIONALLY LEFT BLANK

V. AN APPLICATION OF SOCIOTECHNICAL IDENTITY TO HOMELAND SECURITY

A. ISIS IS A RICH SOCIOTECHNICAL ECOSYSTEM

ISIS has frequently been characterized as having changed the terrorism landscape and for deriving its success from its adoption of emerging technologies. Despite ascribing to a similar extreme Salafist ideology as Al-Qaeda, ISIS has risen to rapid prominence as a fast growing, internationally recruiting, and superlatively wealthy terrorist organization.

During a counterterrorism conference in New York City on December 16, 2015, Federal Bureau of Investigation (FBI) Director James Comey said, "the Islamic State has 'revolutionized' terrorism by seeking to inspire small-scale individual attacks around the world through social media, encrypted communications and slickly produced propaganda."[109] ISIS, or Daesh (used interchangeably), has also been very efficient at leveraging the power of technology to attain its organizational goals. The adoption of certain technologies has also influenced the development of organizational identity. This example explores how ISIS operates as a sociotechnical ecosystem. Then, further analysis assesses the influence ISIS has had by leveraging digital technologies to carry out its objectives of recruitment and propaganda. Following the social identity theory framework, this thesis tests a new framework for sociotechnical identity. Finally, this chapter presents a conjecture regarding the effect technology has on influencing the behavior of the organization and the nature itself of terror attacks.

1. ISIS: A Sociotechnical Ecosystem Dependent Identity

ISIS has become a champion at mass communication. The organization's use of Twitter, Facebook, YouTube, and other social media and web platforms has greatly contributed to its growth and success. ISIS has more than 30,000 human active supporters on Twitter contributing to the information war it is waging in favor of the establishment

[109] Reuters, "Islamic State Has 'Revolutionized' Terrorism: FBI Director," *Newsweek*, December 16, 2015, http://www.newsweek.com/islamic-state-has-revolutionized-terrorism-fbi-director-405968.

of a "caliphate."[110] Twitter has engaged in the suppression of Daesh communications on the social media platform by deleting any account it identifies as belonging to or supporting the mission of the terror group. Yet despite its best attempts, Twitter has struggled to eradicate the group's use of its platform because the users immediately open new accounts with similar handles and simply shift their defunct network over to a new account. The new account runs until deleted once again and so on.

2. Using Penumbral Open Source

ISIS also has developed and disseminated a communication training manual on the open web. This manual describes all the resources available for covert communication, web and data encryption, secure data storage, and geo-location manipulation.[111] Additionally, it offers systematic procedures for dozens of encrypted and deep web browsers. The document also provides information using a suite of text, voice over IP, email, and data storage applications on iOS and Android platforms. Another highly effective method ISIS has been using for communications is MMOGs. Inside virtual worlds like World of Warcraft or Second Life, the organization has found ways to conceal messages as text, voice over IP, or other environmentally compatible methods to communicate unnoticed.[112] In these nearly untraceable environments, imagination alone seems to be the limit, but a deep knowledge of the ecosystem is requisite to engage in hacking a system of sociotechnical clusters for innovation. The direct result of ISIS's preferential ecosystem has been a shift in the archetypical social identity of its membership. The average recruit is 26 years old, male, and fluent in computer-mediated technologies like social-media. This is a stark contrast to Al-Qaeda's recruiting targets that predominantly consisted of status deprived young males who were often illiterate.

---

[110] J. M. Berger and Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter* (Washington, DC: Center for Middle East Policy at Brookings, 2015).

[111] The ISIS covert communication manual is available in digital format at http://justpaste.it/l72d.

[112] Philip Ross, "Terrorists May Have Used PlayStation 4s to Plan ISIS Paris Attacks. Here's How," Free Republic, November 15, 2015, http://www.freerepublic.com/focus/chat/3360820/posts.

With regard to the SIT framework, the capacity for ISIS to communicate internally and to disseminate its global messaging represents a limited good as a result of intelligence interceptions, blocked access to communication platforms, geographic distance to certain interlocutors, and language barriers to potential recruits. Communication as a limited goods exerts a strong constraint on the composition of the organization because the sociotechnical ecosystem demands prerequisite technological knowledge of its prospective recruits, who may be harder to find. This raises an important consideration in the evolution of sociotechnical ecosystems regarding how open or closed sociotechnical ingroups are. I call this property of an ecosystem its technological permeability. Barriers of assimilation to an ingroup have often been based on nationality, religion, political, or economic preference, or other intangible ingroup characterizations, but the organizational technicity of each ingroup also drives the access to group membership.

While belief systems can be aligned with any group's narrative, they do not guarantee a shared social identity absent a technological alignment as well. Some people may have a passion for photography and select to use film in their cameras for the high resolution of the photographs, but despite being part of a photographer ingroup, they come to represent an outgroup to digital photographers. A compelling example of this in the context of conflict is the social identity imparted by the type of explosive artifact some combatants select. While the physics of potential and kinetic energy in a military explosive and an improvised explosive device (IED) may be identical, the connotations on social identity are categorically opposite. The use of an IED may be a quintessential terrorist identity marker while manufactured bombs often tend to support the legitimacy of their users despite a similar capacity for destruction. This nuance of artifact has occasionally been used as an argument to distinguish morality in the Israeli-Palestinian conflict, for example. The object in this case, not the person, drives the perception of social identity. Clandestine communication methods may impart similar labeling.

Understanding how complex a sociotechnical ecosystem is and what barriers to technological adoption a group may confront can provide valuable insight into the permeability or barriers to a particular social identity. The permeability of an ecosystem

appears to be a function of how vulnerable the network is to vertical disruption, how specialized the requisite technicity defining the system is, and how scarce the sociotechnical dimensions are within that system. In the case of ISIS, the organization aims to maintain a balance between the need it has to populate its ranks without providing too much openness, which could facilitate the targeting and elimination of its leadership. Counterterrorism efforts have successfully placed barriers to the communication, mobility, artifacts, and network structure of prior Salafi-jihadist groups like Al-Qaeda; therefore, ISIS has selected to replace those dimensional needs with a virtualization and decentralization of its sociotechnical ecosystem. Protecting the top of the hierarchy requires a reduction in ecosystem permeability, but its survival depends on sustaining or developing the number of members in the lower layers of the organization. For this reason, lower ranks are typically subject to more permeability and function as the gateway to the ingroup while the leadership enjoys a digital divide to buffer and protect their lives. To accomplish both these goals simultaneously, ISIS has created a form of digital jihadist franchise open to the world and managed through the web.

B. WEB 3.0, THE DISTRIBUTED SAFE HAVEN

ISIS has been highly effective at disseminating viral videos of beheadings, mass executions, and other acts of violence to the general public through online video platforms. By combining the use of social media applications, ISIS has nearly eliminated the need for brick and mortar infrastructures, thereby reducing costs, immobility, and vulnerability of targeting. By using Facebook as a recruitment platform, Twitter as a communication tool, and YouTube as its training center, ISIS has been able to shape itself into a "cyber safe haven" for online terrorist development.[113] By comparison, Al Qaeda invested heavily in a static infrastructure of Afghan and Pakistan based terror camps, while ISIS focused on greater agility, mobility, and a broader global reach for membership through free digital communication platforms. While Al-Qaeda conducted mostly covert recruitment from word-of-mouth and through family networks, ISIS has

[113] Geoff Dean, Peter Bell, and Jack Newman, "The Dark Side of Social Media: Review of Online Terrorism," *Pakistan Journal of Criminology* 3, no. 3 (2012): 103–122, http://www.pakistansocietyofcriminology.com/publications/2012_08_10_4110.pdf#page=117.

chosen to come out in the open and cast a global net for recruitment. ISIS was initially faced with limited goods in terms of financial resources and exchange, mobility, communication, and growth of its network. Since then, the organization has shifted the sociotechnical dimensions traditionally used to accomplish the tasks of recruiting, training, and equipping new members of the ingroup, such as providing weapons, establishing new methods to disseminate knowledge, using face-to-face recruitment, and requiring travel to new methods of accomplishing similar goals all within the communication dimension of the ecosystem. As a result, the pool of potential recruits expanded from local villages to the entire globe.

Next, ISIS eliminated the concentration of resources into an easy geographic counterterrorism target by decentralizing the organization, while the cost of information and artifact acquisition was passed on to self-selected global volunteers. This shift in prioritization of the communication dimension for an organization like ISIS resolved many constraints and pressures that Al-Qaeda continues to endure. While Al-Qaeda provides weapons to its combatants mainly in the form of IEDs or suicide vests, ISIS has left the acquisition to its recruits, who favor easily obtainable firearms or vehicles to conduct international attacks. The shift to a decentralized marketing strategy with less direct member oversight comes with a cost though, a reduction in the overall pool of candidates whose technoself profiles are conducive to strong group assimilation. For instance, online recruitment efforts might have been lost to individuals without knowledge or fluency of the deep web or anonymous web browsing.

Unfortunately, in the case of ISIS, the globally cast net flooded a tremendous pool of candidates, increasing the capacity for recruiting and subsequently leading to international attacks. Its success is also tied to the fact that the profile of a typical terrorism candidate is "male, 26, single, quite well-educated but not an expert on the Quran," which characterizes a generation with a strong presence in computer-mediated environments.[114] This digital shift to a decentralized network structure and

[114] Lizzie Dearden, "Isis Documents Leak Reveals Profile of Average Militant as Young, Well-Educated but with Only 'Basic' Knowledge of Islamic Law," *The Independent,* April 21, 2016, http://www.independent.co.uk/news/world/middle-east/isis-documents-leak-reveals-profile-of-average-militant-as-young-well-educated-but-with-only-basic-a6995111.html.

communication model has made it more difficult for traditional human intelligence to intercept, target, and eliminate the growing terrorist group. Additionally, the shift to a stronger presence in cyberspace benefited from the properties of viral sensationalist media. By virtue of the technological shift, terror groups are now more decentralized, socially, ethnically, and politically fluid and increasingly homegrown. ISIS has chosen an asymmetric technological adoption model focused on reshaping its network, simplifying its artifacts, and eliminating mobility needs through emergent means of communication. Its sociotechnical identity is now dependent on and driven by the new constraints of its adapted technological ecosystem.

C. ASYMMETRICAL DISRUPTION—UNRAVELING THE WIRELESS THREAD

#DaeshHunters is the hash tag given to "operation ISIS," a digital war declared by the hacker group Anonymous.[115] According to Anonymous (Anon), its members attacked hundreds of ISIS web assets and deleted thousands of twitter accounts. Anonymous has also conducted "doxing," the online release of personal details, for over 4,000 ISIS members identified through their twitter accounts.[116] So far, the successful counter-operations to the ISIS social media campaign have included the embedding of counter-propaganda videos and links directly onto known ISIS pages, the private sector engagement in deleting ISIS accounts on digital platforms and services, and the activities of hacker groups like Anonymous. The actions undertaken by Anon demonstrate the typical methodological approach to countering the actions and narrative of an identified outgroup by focusing on only one or two dimensions of its sociotechnical ecosystem. The focus on undermining Daesh's activities is concentrated on the communication and information dimensions and has been success in part because of the overwhelming use of computer mediated strategies for all aspects of organizational management. Following the ecosystem perspective proposed in this thesis, we can conclude that the other

[115] Jack Fenwick and Oli Smith, "Anonymous Destroy ISIS Twitter Accounts in Campaign U.S. Officials Take 'Secret Pleasure' In," *Express*, November 19, 2015, https://www.express.co.uk/news/world/620184/ISIS-anonymous-paris-attacks-ISIL-IS-islamic-state-Abdelhamid-Abaaoud-scott-terban.

[116] Danny Yadron, "Anonymous's Hackers Targeting Islamic State Online," *WSJ Online*, November 19, 2015, http://www.wsj.com/articles/anonymouss-hackers-targeting-islamic-state-online-1447881328.

dimensions neglected in “operation ISIS” become an attractor to innovation securing the survival of the organization. The consequence of a digital attack on the social media global outreach of ISIS through hacking by Anon has been a shift in organizational strategy by ISIS to refocus on gaining territory locally, reducing its online presence, and recruiting youth in its controlled territories rather than online.

D. SIZE DOES NOT MATTER: A HUNDRED-POUND ROCK AND A HUNDRED ONE-POUND ROCKS

It is now very clear that ISIS has significantly altered the use of technology for terrorist means. As identified earlier in this thesis, ISIS has harnessed technology and social media to pursue its goals. It seeks to achieve this by publicizing its mission, its methods, and its propensity for violence by making its resources and training manuals open source for crowd-sourcing militants, by hijacking the power of legitimate and influential brand recognition, and by trying to compete with glamorous productions for sensationalism and media attention. Because of this full-spectrum, digital commitment, the technology has become a force driving and shaping the nature, scope, and size of terror attacks giving the organization maximal impact.

Social media has become a force multiplier to the collective psychological internalization of attacks rooted in radicalization and support for ISIS. By leveraging the power of mobile trend monitoring through the viral spread of Twitter, Instagram, and Facebook posts, ISIS is capable of triggering a voyeuristic obsession by social media users with even the smallest acts. Small attacks, which in the past may have only been covered by local news or a brief segment at the national level, now become a national or even global real-time, omnipresent, and digitally proximate experience for even minor events. In turn, this makes the media consumers, now a large swathe of the global population, feel as if they were themselves under the threat of constant attack. This places a fearful and voyeuristic population into a new social identity group of self-categorized, potential victims. Attestation of this is the fact that global sentiment suggests we are in some of the worst, most violent and dangerous times, while data points to a different

reality.[117] Collectively, we now live in some of the most peaceful and safest times in history, but the exposure to conflict is on an order of magnitude greater than at any other time. The greater crisis faced today seems to be the ubiquity and reproducibility of the informational dimension surrounding conflicts and terrorism rather than the absolute value of events.

[117] "Vision of Humanity," Static, accessed March 11, 2017, http://static.visionofhumanity.org/#/page/indexes/global-peace-index.

VI. RECOMMENDATIONS FOR HOMELAND SECURITY IN FUTURE STUDIES OF IDENTITY

While exploring what conclusions to distill from the work and ideas presented in this thesis, I uncovered several proximate ideas, which I give brief consideration hereafter. Subsequently, I draw a much less obvious and more ominous thought that orbits the concepts of social engineering and manipulation. It represents the peak of this conclusion.

A. PRELIMINARY CONCLUSIONS

Understanding the relationship between people and technology provides insight into opportunities for technological innovation, risks of unintended consequences, and opportunities for disrupting undesirable human behaviors by undermining the technological crutches facilitating their actions. The concept and framework of sociotechnical ecosystems is important to understanding how people and technology respond to their environment and how that in turn shapes human behavior and therefore sociotechnical identity.

1. A Novel Framework

The holistic sociotechnical ecosystem framework entwining artifact, mobility, communications, information, and human network structures into a cognitive toolkit for understanding dynamic identity can play a vital role in enhancing the development of programs to support social integration and reduce the propensity of certain individuals toward radicalization and extremism of disaffected youth. It also allows counterterrorism professionals to study and then develop strategies focusing on the most relevant sociotechnical dimensions to disrupt terrorism and organized violence, while remembering that an ecosystem is a continuously adapting system.

The framework may provide direct benefits such as facilitating the understanding of how humans manipulate, hack, and develop technology to enhance certain sociotechnical pursuits. This offers insight into the potential unintended consequences of technological innovation by delineating a perimeter of potential repurposing or

unexpected social interactions for any given technology. It also can improve the understanding of what social groups aim to accomplish or improve through the use of technology, thereby giving innovators and organizations insightful opportunities and direction for future technological inventions by playing on sociotechnical dimensional gaps and the recombinant nature of technology.

In the context of conflict, technology is directly connected to the value and impact of attacks; therefore, it enables a transformation in the nature of these attacks to take place without jeopardizing their dissemination and influence on society. Following this logic and associated with the formation of a cyber safe-haven for online terrorism, we can project that the era of expensive, complex, and large attacks like 9/11 will decline and that the future of terrorism is the small, decentralized, "independent contractor" or lone-wolf type attacks spread around the world. Decentralizing and franchising terrorism and its organizations is cheaper, logistically easier, and more difficult for counterterrorism organizations to identify and track. It allows an increase in the frequency of events, yet it does not seem to compromise the sought impact or attention thanks to the viral media magnification of technology.

We are clearly at a technological crossroads in which humans and technology share an inextricable ecosystem. This ecosystem perspective has major ramifications for terrorism recruitment, outreach, attacks, and future study. This framework leads to two emergent considerations requiring further study. The first is whether the social identity theory should migrate toward a sociotechnical approach to studying social categorization and social dynamics, and the second is the need to explore the influence a personified technology has on the practice of terrorism itself. As FBI Chief Comey stated, ISIS, perhaps a bit untowardly, has revolutionized terrorism by adopting and leveraging technologies capable of themselves transforming terrorism.[118]

Another interesting finding that has emerged in developing the concept of a sociotechnical ecosystem as well as ideas regarding sociotechnical identity has to do with unintended consequences following the adoption of emerging technologies. If group

[118] Reuters. "Islamic State Has 'Revolutionized' Terrorism."

identity is defined in part by the technology it adopts and adapts to fulfill existing and emerging needs, then the application of those technologies transform the outcomes beyond the intended design. This expected use leads to anticipated outcomes, but it sometimes can result in unintended consequences—as either positive or negative innovations. What this means is that if a sociotechnical ecosystem defines the boundaries of the technicity of a system, then the unintended consequences of technological applications will fall within these boundaries and will affect one or more of the dimensional boundaries. If this is true, then we can use a systematic approach, just as is suggested for social behavior and intergroup conflict, to evaluate and anticipate the possible unintended consequences of technological use.

2. The Customization of Sociotechnical Identity

The observations in this thesis of the interplay between humans and the technium have made it clear that technicity and technological innovation have had a significant impact on altering social behavior and identity, although it still seems to be quite involuntary or accidental. The focus and attention given to discussions and research surrounding the unintended consequences of technological innovation show that we still focus on the resultant influences of adopted technologies outside their narrowly intended purposes, rather than leveraging the principles of sociotechnical identity to invent and design with intended consequences on identity. We have always intuitively known that technology fulfills an intended function and purpose, a means to an end, and that it systematically forces a change in human behavior, which then in turn modifies self-perception and ultimately identity. The drive toward technological innovation has generally missed its capacity to alter human identity by intelligently embedding a capacity for adaptation within the developed tools or by holistically planning the configuration of all dimensions of social influence existing within the technium.

If we take the strategy of using drone attacks to eliminate the leadership of a terrorist organization, such as ISIS, it is easy to see that the targeting of the terrorist group’s sociotechnical ecosystem focuses predominantly on altering its network structure by eliminating people in leadership positions. This also alters part of the ingroup

information by eliminating established goals, objectives, and purpose and the group's capacity for a hierarchical communication geometry on which orders and strategic guidance are dependent. The direct effects of a strategy to topple leadership in the context of ISIS, for example, has resulted in the terror group's focus on innovation in the mobility and artifact dimensions and adaptation in network structures, information, and communication. These pressures have driven much of the differences we see between Al-Qaeda and ISIS. Also, this has in part led to the greater resilience of ISIS over the former by modifying the sociotechnical ecosystem to a decentralized, internationally reaching, strong online community that is less interested in complex coordinated terror attacks with engineered multicomponent weaponry than in the convenience and social media virulence of franchised random radical actors. Complex coordinated terrorist attacks require too much highly vulnerable logistical interplay to carry out with a high degree of confidence, so the change in the terrorist identity of ISIS has itself led to a change in the nature of attacks ISIS carries out internationally. By offering a terrorist franchise opportunity to disenfranchised individuals with no ingroups and strongly undermined social identity, ISIS has harnessed the opportunity afforded by viral and sensationalist media for psychological trauma through logistically simple attacks like mass shootings or vehicles driven through crowds.

The answer to preventing these types of acts of terrorism may lie in the altering and construction of a strong sociotechnical ecosystem in known vulnerable populations. With an understanding of the taxonomy and ontology of sociotechnical ecosystems, it is now possible to analyze, anticipate, and develop technologies with the intent of driving specific identity changes and transformations in people. What homeland security professionals need to take away from the idea of sociotechnical ecosystems is that social technicity and technologies in all five suggested dimensions of the ecosystem have the capacity to authentically and fundamentally alter social identity. The questions become what homeland security needs to do when faced with constant new technological adoption and innovation to protect and preserve identity, as well as how a nation can leverage the influence sociotechnical ecosystems have on identity to detract transnational,

terrorist, or criminal actors susceptible to radicalization from adhering and belonging to those types of groups.

The fundamental intention of this thesis is not to think of technology in terms of the potential threats it may present to critical infrastructure, privacy, or user safety but rather the important influence it has on identity itself. Rather than focusing on the unintended consequences of technology, homeland security should consider studying the intended consequences of technology on human identity with a deep consideration of how it can be leveraged to undermine national and group identity, how it influences individual identity and psychological well-being, and finally maintaining a sharp focus on understanding all the ethical implications of sociotechnical innovation and design used to alter human identity.

B. EPILOGUE

In this section, I address subjects worthy of attention in the context of this thesis but which do not tie neatly into the necessary discussion of the core question. Nonetheless, these next few topics demand mention and will surely lead to future exploration.

1. A Short Series of Loose Ends and Future Explorations

Ingroups are generally formed by individuals adhering to a common narrative or identity, but these groups may become divided simply because of the technologies adopted within the group. An example of this is the phenomenon observed by Stephen Graham and Simon Marvin; they name it *splintering urbanism.*[119] The theory of splintering urbanism involves the "fragmentation of the social and material fabric of cities" into "cellular clusters of globally connected high-service enclaves and network ghettos" driven by electronic networks that segregate as much as they connect.[120]

[119] Simon Marvin and Stephen Graham, *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition* (London, UK: Routledge, 2001), 52.

[120] *Wikipedia*, s.v. "Urbanism," August 29, 2016, https://en.wikipedia.org/w/index.php?title=Urbanism&oldid=736793023.

a. Technarianism

The construction of neighborhoods, varying architecture, and the concentration and availability of critical urban resources and infrastructure all play a key role in shaping identity by molding the space and environment people use to live in, travel, and work. This is best illustrated by the predominant segregation of cities into culturally, racially or financially homogenous neighborhoods such as financial districts, Chinatowns, or ghettos. Moving from this example of the urban environment to the more general concept of sociotechnical ecosystems, it becomes clearer that group splintering can either be an unintended consequence of the adoption of new technologies or can be the result of an intentional introduction of subversive technologies placed to transform a loosely connected ingroup into several more tightly linked ingroups. This phenomenon, leading to the splintering of social groups through the evolution of socially adopted technologies, can be leveraged to optimize recruitment as ISIS has done. This was accomplished by baiting video-game addicted western youth to join a high-paced real-world equivalent environment. It can also form a sociotechnical divide between groups like ISIS and Al-Qaeda by injecting competing network structures, communication modalities, an artifact of social typography, and highly differing narratives. This phenomenon can be leveraged as an important tool in countering radicalization, violent extremism, or other threatening behaviors, but presents potential social engineering threats as mentioned previously.

b. Biotechnology

Advances in biotechnology and biocomputation, as touched upon in this thesis, are also feeding the growth of sociobiological influences on identity. The idea of a physiology of technology pertains to the functions of technology on the social body. The risks that emerge when intentionally manipulating technology for the purpose of controlling social identity could lead to something I call *eutechnics*. The idea spins on a deification of emerging technologies as a new supreme and primordial state allowing deeper insight into the world. Some religious groups, such as evangelicals, have started endorsing gene therapy, giving a theological justification to genetic engineering and augmented technologies. The cypherpunk movement endorses strong cryptography and

privacy enhancing technologies, which if applied maliciously could deprive individuals from access to their own trove of indispensable biometrics. Although this is in contrast to the stark evolutionary bias of eugenics during Nazi Germany, the idea of technologically based supremacy, eutechnics, could emerge as the root motivation behind a subnational global cyber warfare or a supremacist hacker group attacking critical infrastructure to undermine the cyber illiterate majority. Organized crime syndicates and mobs could shift from thugs to bugs to sustain organizational sustainability.

The power of technological forces in the sociotechnical paradigm is their ability to influence individuals and groups through cognition as well as through growing biological means. Technology holds tremendous power in its ability to modify behavior simply through its users' perceived experience of reality. Therefore, it is much clearer how critical our ability to understand the biological influence technological innovation and evolution will play on human behavior. With sociological desires and competition steering the direction of technological innovation, we should anticipate a growing trend toward the pursuit of biological and sociological control mechanisms through technological means. In considering how the discipline of public health studies epidemiology, behavioral health, or pathogenesis, for example, and subsequently establishes controls and policies to modify human behavior through vaccination, quarantine, or consumption laws, it is interesting to consider whether technologies will eventually be identified as posing important sociological risks and subsequently require policies to control and modify sociotechnical behaviors.

With the spread of the Internet of Things into all aspects of the social fabric, the use of nanoprocessors or microcontrollers will not simply control the devices they are embedded in but will eventually also control the behavior of those enveloped in the social networks of meshed feedback systems. Human trust used to be something conferred upon other humans after long meaningful relationships developed over time; now a simple and poorly programed GPS can direct someone to drive off a cliff.[121]

[121] Sara Wolfe, "Driving into the Ocean and 8 Other Spectacular Fails as GPS Turns 25," Public Radio International, February 17, 2014, https://www.pri.org/stories/2014-02-17/driving-ocean-and-8-other-spectacular-fails-gps-turns-25.

2. Future Ecosystems

In 1984, William Gibson described cyberspace in the following way.

> A consensual hallucination experienced daily by billions of legitimate operators, in every nation... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters, and constellations of data. Like city lights receding.[122]

In the contemporary digital paradigm it is simple to find support for both constructivist and deterministic currents, but when considered holistically, the digital environments contained within the Internet, consist of a complex technologically influenced social paradigm. Terms like *Internet*, *the web*, *online*, *digital worlds*, *virtual worlds*, *virtual reality*, or *cyberspace* can denote some specific aspect of the emerging technological space, but in this context, they are considered interchangeable and refer to any "computer-mediated environment."[123]

This online environment is important to this discussion because it is frequently described as generating a phenomenological experience of authentic reality in its users.[124] This makes it an essential space to study in the sociotechnical ecosystem context because it offers more versatility in self-presentation and social interactions than in real-world, face-to-face environments. Much of the appeal generated in digital representations of the self comes from the lack of physiologically bound assumptions about identity. Online, it is easier to represent oneself according to an identity marker unsupported or in opposition of one's physical characteristics. The appeal is in the capacity to disrupt and replace ascribed one's identity with an avowed self-presentation. Consequently, the way groups develop and interact as well as the possibilities for defining personal identity have become boundless. It is important to understand that from a sociological perspective, cyberspace is much more than a specific technological device or system. Rather, it is a subset of socially constructed reality with its own emerging technicity and phenomenon

[122] William Gibson, *Neuromancer* (New York: Ace, 1984), 51.

[123] Donna Hoffman and Thomas Novak, "Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations," *Journal of Marketing* 60, no. 3 (1996): 50–68.

[124] Paul Szoldra, "It's Nearly Impossible to Describe the Mind-Blowing Experience of Virtual Reality," *Business Insider*, February 10, 2016, http://www.businessinsider.com/virtual-reality-is-2016-2.

free of physical and biological boundaries. It is an ecosystem wherein the fantastical and the imagined take form and can in turn cause direct consequences on the physical world. In the context of homeland security, this opens to a panoply of new threats to economic integrity, critical infrastructure, and human safety and security. The digital universe has completely expanded the boundaries of sociotechnical reality by creating a universe in which information is inherently free to take any *metaform*, in which the space hosts any representation of reality, and it offers a boundless environment in which to project the pursuit of identity.[125] Online, people are free to curate and reinvent themselves in any way they want.

These virtual realities are a critical piece of the sociotechnical ecosystem discussion as they offer a new experiential space made up of synthetic phenomena that redefine the human experience. This offers a new alternative to the natural phenomena of the physical analog reality where we ordinarily confine the idea of technicity. If we consider physiological effects on the body, such as the vertigo or fear that a virtual reality headset can trigger by placing the user on a hundred-foot ledge or in a snake pit, we come to realize that the impact of synthetic phenomenon can be physiologically indistinguishable to the user from the natural phenomenon of the physical world. For this reason, it is important to consider digital reality not as a piece of technology but rather as a legitimately perceived layer of socially constructed reality. This new boundless reality, uncontained by natural limits or the ability to discern truthfulness, can influence human behavior in negative or dangerous ways.

In *The Presentation of Self in the Online World,* Bullingham and Vasconcelos discuss Goffman's work on identity presentation and apply it online in the context of blogging and the MMOG Second-Life.[126] Their analysis looked at 10 cases focusing on "expressions given; embellishment as a minor form of persona adoption; dividing the

[125] The term *metaform* is proposed here to represent any virtual representation, whether real, invented or metaphorical, of real-world people, places, products or properties.

[126] Liam Bullingham and Ana C. Vasconcelos, "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities," *Journal of Information Science and Engineering* 39, no. 1 (2013): 101–112.

self; conforming and 'fitting in;' and masking, anonymity and pseudonymity."[127] What they found is that participants did not engage in "whole persona adoption," but rather they constructed enhanced versions of their offline selves to improve their online presentation.[128] Having altered their self-representation to others, they are willing to accept masked, anonymous, and pseudonymous identities as acceptable representations of another person's identity with which they may interact. In turn, that other participant may modify and conform their own identity to fit the ingroup by again dividing the self and embellishing their personas to outmatch pseudonymous personas. As members repeat the process, they soon find themselves pushing their identity boundaries beyond their real-world limits. This phenomenon can lead to the escalation of behavioral and discursive norms within an online group resulting in extremism, violence, or crime.

For homeland security, the concern with MMOGs, virtual ecosystems, and online forums is that they can facilitate pervasive explorations of online identity and foster both online and offline social cohesion by bringing physical participants together at conventions or protests, for example. When introduced in the offline space, some individuals with extreme viewpoints developed online can meet and subsequently form a social group built on an unnatural ingroup narrative rooted in the original relational anonymity. Consequently, the fact that online social interactions facilitate a narrative synergy that would not otherwise exist offline should be of great concern to the discipline of homeland security.

One example of the potential narrative escalation emerging from the Internet is the Alt-Right movement that was established by Richard Spencer in 2008 following the growth of white nationalist discourse by American internauts[129] since the second

[127] Ibid.

[128] Ibid.

[129] The oxford dictionary defines an internaut as a portmanteau of the words internet and astronaut. It refers to habitual or competent users of the internet.

invasion of Iraq.[130] Breitbart, a media outlet familiar with Alt-Right views, described the movement in the following way:

> the alt-right is a movement born out of the youthful, subversive, underground edges of the internet. 4chan and 8chan are hubs of alt-right activity. For years, members of these forums—political and non-political—have delighted in attention-grabbing, juvenile pranks. Long before the alt-right, 4channers turned trolling the national media into an in-house sport.[131]

The consequences of this anonymized social play in the deep web was the eventual emergence of a white nationalist movement that has subsequently secured itself a role in the U.S. political establishment.

a. Digital Communities

The following section further explores virtual ecosystems to identify markers of sociotechnical influence much in the way actor network theory, constructivists, or determinists study the mutual influences of technology and people offline. According to Ted Lewis,

> Whether in advertising, marketing of websites, promotion of political campaigns, or simply understanding the dynamics of socio-political movements around the globe, flashmob behavior modification is a matter of pulling the right levers. Mob formation has little to do with human nature and psychology, and much to do with conviction and the inclination of your neighbors. Power and influence is a mechanical property of boulevardiers, activists, and trendsetters. Persuasion can be had simply by shaping the typology of the network. Function follows form.[132]

Nothing has made this statement more convincing than the development and utilization of social media platforms like Twitter and Facebook. These digital social ecosystems have categorically transformed the typology of certain social networks from traditional hierarchical structures to scale-free networks of spontaneous and transitive participants.

---

[130] Jessica McBride, "What Is the Alt Right? 5 Fast Facts You Need to Know," *Heavy*, November 18, 2016, http://heavy.com/news/2016/11/alt-right-trump-alternative-white-nationalist-reddit-website-memes-what-is-it-definition-meaning-donald-steve-bannon-twitter-ban-nazi/.

[131] "An Establishment Conservative's Guide to the Alt-Right," *Breitbart*, March 29, 2016, http://www.breitbart.com/tech/2016/03/29/an-establishment-conservatives-guide-to-the-alt-right/.

[132] Lewis, *Book of Extremes*, 32.

While pre-Internet social ingroups formed gradually around common grievances, eventually resulting in organized and premeditated protests, today's protests appear to form nearly spontaneously online shaped as leaderless organizations, free of the prior geographic imperatives, and with a great diversity in its participation. A clear example of this tendency is the Occupy movement with the "We are the 99%" slogan, which followed the Occupy Wall Street protest started in September of 2011. What started as an online call to action by the Canadian anticonsumerism publication, *Adbusters*, against wealth and income inequality rapidly turned into a global movement of peaceful protests, occupations, civil disobedience, picketing, and Internet activism resulting in everything from arrests to changes in political power.[133]

The creation of online social networks to facilitate and support the social imperative to connect with others fulfills the constructivist argument while the emergent availability of digital means to connect, organize, and communicate outside the boundaries of real-world sociopolitical constraints supports the deterministic school. The existence of the Internet has facilitated the development of new virtual social entities bound by emergent languages, common interests and perspectives, or by offering an alternative environment to reunify socially or physically displaced populations into digital communities, nations, and diasporas. In this way, cyberspace is inviting the development of new ethnopolitics, social behaviors, and virtual social identity, all of which have implications on the study and practice of homeland security.

b. The Metaverse

What the Internet is facilitating is the emergence of a multidimensional reality, wherein geopolitics, social identity, and the iterations of a "self" are entraining a new global *metasystem*, composed of the physical and virtual worlds and breaking down the barriers of nationality, age, gender, and to a certain extent, socioeconomics. The world is witnessing the development of a set of parallel realities akin to Neal Stephenson's 1992

[133] *Wikipedia*, s.v. "Occupy Wall Street," *The Free Encyclopedia*, November 20, 2016, https://en.wikipedia.org/w/index.php?title=Occupy_Wall_Street&oldid=750477664.

concept of a "Metaverse."[134] In their work on virtual social identity, Ebrahimi and Salaverría described Stephenson's metaverse as

> the complicated marriage of everyday mundane life with a fantasy world in which an inhabitant assumes other identities [that] opened the door to thoughts of digital social experimentation—and presented a pathway to self-aggrandizement for those whose "real-world" lives is less than ideal.[135]

When individuals begin creating a curated representation of themselves in virtual reality and perceive their avatars as a more appropriate representation of who they really feel they are, questions immediately ensue regarding the legitimacy, validity, and authenticity of the digital identity as an extension of a human. Ironically, people are simultaneously relying more heavily on digital forms of identification, such as biometrics, to determine and validate actual identity while also free to completely fabricate and invent new selves using digital technologies. In digital ecosystems, these identities, both validated and fabricated, are also subject to theft in ways that are impossible offline. While the theft or intentional damaging of a physical possession or technology, like the computer through which a victim controls his or her virtual identity, is protected by the legal system, there is little clarity on the implications and consequences of a malicious actor hacking, damaging, stealing, altering, violating, or shaming someone's virtual identity. Similarly, if an individual or a group develop a virtual representation of someone else's identity for the purposes of publicly shaming him or cyber-bullying her, possibly resulting in the victim's suicide, there is limited consensus as to how these cases must be addressed. This certainly results from the lack of understanding or specific definition of sociotechnical identity.

What has become clear is that unique sets of real-world safety and security concerns are emerging as a result of the sociological influence of digital ecosystems. Whether it affects people's sense of identity, immigration, terrorism, social movements, or revolutions, the virtual ecosystem presents unique homeland security challenges that

---

[134] Neal Stephenson, *Snow Crash* (New York: Bantam-Random, 1992).

[135] Natalie Wood and Michael Solomon, *Virtual Social Identity and Consumer Behavior* (New York: Routledge, 2014).

still lack a systematic framework for analysis. Furthermore, this ecosystem invites people to transcend their own biological limits in pursuit of their technoselves, raising new questions regarding both avowed and ascribed identity. Much of the gap in analytical methodology to study these sociotechnical ecosystems, and particularly the emerging digital ecosystems just identified, result from a limited ontological understanding of technicity combined with a technological capacity to redefine identity in modern times. It is no longer just the technology that people use that can be hacked but the very people themselves. Consequently, what we believe we currently know about social identity is shifting toward obsolescence.

LIST OF REFERENCES

92Y Plus. “Brain Jazz: A Mind-Jam with Jason Silva and Douglas Rushkoff.” YouTube. January 2, 2014. https://www.youtube.com/watch?v=HTP0NQlyB3w.

Abrams, Dominic, and Michael A. Hogg. “Comments on the Motivational Status of Self-Esteem in Social Identity and Intergroup Discrimination.” *European Journal of Social Psychology* 18, no. 4 (1988): 317–334.

Ardrey, Robert. *The Hunting Hypothesis: A Personal Conclusion Concerning the Evolutionary Nature of Man*. London: Macmillan Pub. Co, 1976.

Arthur, Brian W. *The Nature of Technology: What It Is and How It Evolves*. New York: Simon and Schuster, 2009.

The Atlantic. “Attention, Employers: Millennials Have Made Their Demands.” Accessed January 15, 2017. http://www.theatlantic.com/sponsored/allstate/attention-employers-millennials-have-made-their-demands/219/.

Barrell, Ray, and Tatiana Fic. “Integration, Globalisation, Technology and Trade Patterns in the EU8.” *Research in Economics and Business: Central and Eastern Europe* 2, no. 1 (2013): 34–46. http://rebcee.eu/index.php/REB/article/view/23.

Beard, Charles A. “Time, Technology, and the Creative Spirit in Political Science.” *The American Political Science Review* 21, no. 1 (1927): 1–11.

Badham, Richard, Chris Clegg, Toby Wall. “Socio-technical Theory.” In *International Encyclopedia of Ergonomics and Human Factors*, edited by Waldemar Karwowski, 1370–1374. New York: Taylor and Francis, 2001.

Berger, J. M., and Jonathon Morgan. *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*. Washington, DC: Center for Middle East Policy at Brookings, 2015.

Berger, Peter, and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. London UK: Penguin Books Ltd, 1966.

Bijker, Wiebe E., Thomas P. Hughes, and Trevor J. Pinch, eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987.

Bostrom, Nick, and Anders Sandberg. *The Future of Identity*. London: Future of Humanity Institute, Oxford University, 2011. http://www.nickbostrom.com/views/identity.pdf.

Brannan, David W., Kristin M. Darken, and Anders Strindberg. *A Practitioner's Way Forward: Terrorism Analysis.* Salinas, CA: Agile Research and Technology, Incorporated, 2014.

Breitbart. "An Establishment Conservative's Guide to the Alt-Right." March 29, 2016. http://www.breitbart.com/tech/2016/03/29/an-establishment-conservatives-guide-to-the-alt-right/.

Brynjar, Lia, and SkjØlberg Katja. *Causes of Terrorism: An Expanded and Updated Review of the Literature*. Kjeller, Norway: Norwegian Defense Research Establishment, 2004. https://www.ffi.no/no/Rapporter/04-04307.pdf.

Bullingham, Liam, and Ana C. Vasconcelos. "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities." *Journal of Information Science and Engineering* 39, no. 1 (2013): 101–112.

Chien, Jui-Pi. "Umwelt, Milieu (X. and Environment: A Survey of Cross-cultural Concept Mutations." *Semiotica* 2007 no. 167 (2007): 65–89. http://philpapers.org/rec/CHIUMA,

Dean, Geoff, Peter Bell, and Jack Newman. "The Dark Side of Social Media: Review of Online Terrorism." *Pakistan Journal of Criminology* 3, no. 3 (2012): 103–122. http://www.pakistansocietyofcriminology.com/publications/2012_08_10_4110.pdf#page=117.

Dearden, Lizzie. "Isis Documents Leak Reveals Profile of Average Militant as Young, Well-Educated but with Only 'Basic' Knowledge of Islamic Law." *The Independent*, April 21, 2016. http://www.independent.co.uk/news/world/middle-east/isis-documents-leak-reveals-profile-of-average-militant-as-young-well-educated-but-with-only-basic-a6995111.html.

Descartes, René. *René Descartes: Meditations on First Philosophy: With Selections from the Objections and Replies*, edited by and translated by John Cottingham. Cambridge: Cambridge University Press, 2013.

Eagleman, David. "The Umwelt." *David Eagleman* (blog. 2012. http://www.eagleman.com/blog/umwelt.

Eason, Ken. "Sociotechnical Systems Theory in the 21st Century: Another Half-Filled Glass." In *Sense in Social Science: A Collection of Essays in Honour of Dr. Lisl Klein*, edited by Desmond Graves, 123–134. Mulgrave, Victoria: Broughton, 2008. http://static1.1.sqspcdn.com/static/f/632322/9574694/1290775147427/Sociotechnical+systems+theory+in+the+21st+Century.pdf?token=Y2DRRODRd4MeBJg9wa%2F2x0L%2B3T8%3D.

Ellul, Jaques. *La Technique Ou L'enjeu Du Siècle* [The Technological Society]. Translated by John Wilkinson. New York: Vintage Books. 1967.

Emery, Frederick Edmund. *Characteristics of Socio-Technical Systems: A Critical Review of Theories and Facts*. London: Tavistock Institute of Human Relations, 1959.

Farmer, David John. *The Language of Public Administration: Bureaucracy, Modernity, and Postmodernity*. Tuscaloosa, AL: University of Alabama Press, 1995.

Fenwick, Jack, and Oli Smith. "Anonymous Destroy ISIS Twitter Accounts in Campaign U.S. Officials Take 'Secret Pleasure' In." *Express*, November 19, 2015. https://www.express.co.uk/news/world/620184/ISIS-anonymous-paris-attacks-ISIL-IS-islamic-state-Abdelhamid-Abaaoud-scott-terban.

Gibson, William. *Neuromancer*. New York: Ace, 1984.

Goga, Oana, Giridhari Venkatadri, and Krishna P. Gummadi. "The Doppelgänger Bot Attack: Exploring Identity Impersonation in Online Social Networks." In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, 141–153. New York: ACM, 2015.

Greenfield, Susan. *Mind Change: How Digital Technologies Are Leaving Their Mark on Our Brains*. New York: Random House Publishing Group, 2015.

Gregoire, Carolyn. "The Internet May Be Changing Your Brain in Ways You've Never Imagined." *The Huffington Post*, October 9, 2015. http://www.huffingtonpost.com/entry/internet-changing-brain-nicholas-carr_us_5614037de4b0368a1a613e96.

Hiscott, Rebecca. "8 Ways Tech Has Completely Rewired Our Brains." *Mashable*, March 14, 2014. http://mashable.com/2014/03/14/tech-brains-neuroplasticity/;

Hoffman, Donna, and Thomas Novak. "Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations." *Journal of Marketing* 60, no. 3 (1996): 50–68.

Ionescu, Ana-Cristina. "Cyber Identity: Our Alter-Ego?" In *Handbook of Research on Technoself*, edited by Rocci Luppicini, 190–203. Hershey, PA: IGI Global, 2012.

Kegley, Charles W. *International Terrorism: Characteristics, Causes, Controls*. New York: St. Martin's Press, 1990.

Kelly, Kevin. *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*. Reprint. New York: Basic Books, 1995.

———. "The Technium and the 7th Kingdom of Life." Edge. July 18, 2007. https://www.edge.org/conversation/kevin_kelly-the-technium-and-the-7th-kingdom-of-life.

———. “The Technium: The Seventh Kingdom.” KK. February 1, 2006. http://kk.org/thetechnium/the-seventh-kin/.

———. *What Technology Wants*. New York: Penguin Group, 2010.

Klein, Hans K., and Daniel Lee Kleinman. “The Social Construction of Technology: Structural Considerations.” *Science, Technology & Human Values* 27, no. 1 (2002): 28–52.

Koltko-Rivera, Mark E. “Rediscovering the Later Version of Maslow’s Hierarchy of Needs: Self-Transcendence and Opportunities for Theory, Research, and Unification.” *Review of General Psychology* 10, no. 4 (2006): 302–317.

Konrath, Sara. “The Empathy Paradox: Increasing Disconnection in the Age of Increasing Connection.” In *Handbook of Research on Technoself,* edited by Rocci Luppicini, 204–228. Hershey, PA: IGI Global, 2012.

Kurzweil, Ray. *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. New York: Penguin Book, 2000.

———. *The Singularity Is Near: When Humans Transcend Biology*. New York: Penguin Books, 2005.

Lagerspetz, Kari. “Jakob von Uexküll and the Origins of Cybernetics.” *Semiotica* 134, no. 1/4 (2001): 643–651.

Latour, Bruno. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Clarendon Lectures in Management Studies. Oxford: Oxford University Press, 2005.

Law, John. “Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity.” *Systems Practice* 5, no. 4 (1992): 379–393.

Lewis, Ted G. *Book of Extremes: Why the 21st Century Isn’t Like the 20th Century*. New York: Springer International Publishing, 2014.

Luppicini, Rocci. “The Emerging Field of Technoself Studies (TSS).” In *Handbook of Research on Technoself: Identity in a Technological Society*, edited by Rocci Luppicini, 1–25. Hershey, PA: IGI Global, 2012.

———. *Handbook of Research on Technoself: Identity in a Technological Society*. Hershey, PA: IGI Global, 2012.

Lyons-Padilla, Sarah, Michele J. Gelfand, Hedieh Mirahmadi, Mehreen Farooq, & Marieke van Egmond. “Belonging Nowhere: Marginalization and Radicalization Risk among Muslim Immigrants.” *Behavioral Science & Policy* 1, no. 2 (2015): 1–12.

Marvin, Simon, and Stephen Graham. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. London, UK: Routledge, 2001.

Maslow, Abraham. "A Theory of Human Motivation." *Psychological Review* 50, no. 4 (1943): 370–396.

McBride, Jessica. "What Is the Alt Right? 5 Fast Facts You Need to Know." *Heavy*, November 18, 2016. http://heavy.com/news/2016/11/alt-right-trump-alternative-white-nationalist-reddit-website-memes-what-is-it-definition-meaning-donald-steve-bannon-twitter-ban-nazi/.

McCreery, Michael Patrick. "Personality, Presence, and the Virtual Self: A Five-factor Model Approach to Behavioral Analysis within a Virtual Environment. PhD diss., University of Nevada, 2011. http://digitalscholarship.unlv.edu/thesesdissertations/1043.

McLuhan, Marshall. *Understanding Media*. New York: McGraw-Hill, 1964.

Nieto Gómez, Rodrigo. "This Is Your Brain on Code: Embodied Intelligence Augmentation and Conflict." In *Augmented Intelligence: Smart Systems and the Future of Work and Learning*, edited by Daniel Araya. New York: Peter Lang, 2018. Forthcoming.

Noonan, Harold, and Ben Curtis. "Identity." *Stanford Encyclopedia of Philosophy*. April 25, 2014. http://plato.stanford.edu/entries/identity/.

Olson, Eric T. "Personal Identity." In *The Blackwell Guide to Philosophy of Mind*, edited by Stephen P. Stich, and Ted A. Warfield, vol. 9. Blackwell Philosophy Guides. Malden, MA: Blackwell Publishing Ltd, 2003.

Ramachandran, Vilayanur, and William Hirstein. "The Science of Art: A Neurological Theory of Aesthetic Experience." *Journal of Consciousness Studies* 6, no. 6–7 (1999): 15–51, http://www.ingentaconnect.com/content/imp/jcs/1999/00000006/F0020006/949.

Reuters. "Islamic State Has 'Revolutionized' Terrorism: FBI Director." *Newsweek*, December 16, 2015. http://www.newsweek.com/islamic-state-has-revolutionized-terrorism-fbi-director-405968.

Ross, Philip. "Terrorists May Have Used PlayStation 4s to Plan ISIS Paris Attacks. Here's How." Free Republic. November 15, 2015. http://www.freerepublic.com/focus/chat/3360820/posts.

Rushkoff, Douglas. “In a World That’s Always on, We Are Trapped in the ‘Present,’” interview by Audie Cornish, *All Things Considered*. NPR, March 25, 2015. http://www.npr.org/2013/03/25/175056313/in-a-world-thats-always-on-we-are-trapped-in-the-present?sc=ipad&f=1019.

Shapiro, Stuart. “Caught in a Web: The Implications of Ecology for Radical Symmetry in STS.” *Social Epistemology* 11, no.1 (1997): 97–110.

Stephenson, Neal. *Snow Crash*. New York: Bantam-Random, 1992.

Stern, Jessica. “Radicalization to Extremism and Mobilization to Violence: What Have We Learned and What Can We Do about It?” *The Annals of the American Academy of Political and Social Science* 668, no. 1 (2016): 102–117.

Stets, Jan, and Perter Burke. “Identity Theory and Social Identity Theory.” *Social Psychology Quarterly* 63, no. 3 (2000): 224–237. http://wat2146.ucr.edu/papers/00a.pdf.

Szoldra, Paul. “It’s Nearly Impossible to Describe the Mind-Blowing Experience of Virtual Reality.” *Business Insider*, February 10, 2016. http://www.businessinsider.com/virtual-reality-is-2016-2.

Tajfel, Henri, ed., *Differentiation between Social Groups: Studies in the Social Psychology of Intergroup Relations*. London: Academic Press, 1978.

U.S. Department of the Army. *Basic Officer Leader Training Policies and Administration* (TRADOC Regulation 350-36). Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2015. http://www.tradoc.army.mil/tpubs/regs/TR350-36.pdf.

Vojinović, Zoran, and Michael B. Abbott. *Flood Risk and Social Justice: From Quantitative to Qualitative Flood Risk Assessment and Mitigation*. London: International Water Association Publishing, 2012.

Wade, Nicholas. “Your Body Is Younger Than You Think.” *The New York Times*, August 2, 2005. http://www.nytimes.com/2005/08/02/science/your-body-is-younger-than-you-think.html.

Winner, Langdon. “Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology.” *Science, Technology & Human Values* 18, no. 3 (1993): 362–378.

Wolfe, Sara. “Driving into the Ocean and 8 Other Spectacular Fails as GPS Turns 25.” *Public Radio International*, February 17, 2014. https://www.pri.org/stories/2014-02-17/driving-ocean-and-8-other-spectacular-fails-gps-turns-25.

Wood, Natalie, and Michael Solomon. *Virtual Social Identity and Consumer Behavior*. New York: Routledge, 2014.

Yadron, Danny. “Anonymous’s Hackers Targeting Islamic State Online.” *WSJ Online*, November 19, 2015. http://www.wsj.com/articles/anonymouss-hackers-targeting-islamic-state-online-1447881328.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California